NAVAL POSTGRADUATE SCHOOL

Monterey, California

THESIS

INFORMATION RESOURCE MANAGEMENT
ABOARD USS CORINTH (CG-44):
A CASE STUDY

by

LCDR Cheryl L. Gonzalez

March 1991

Thesis Advisor: William J. Haga

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION Unclassified	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S)	5 MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL (*If applicable*) 55	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000	7b. ADDRESS (*City, State, and ZIP Code*) Monterey, CA 93943-5000
8a. NAME OF FUNDING/SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (*If applicable*)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (*City, State, and ZIP Code*)	10. SOURCE OF FUNDING NUMBERS Program Element No / Project No / Task No / Work Unit Accession Number

11. TITLE (*Include Security Classification*)
INFORMATION RESOURCE MANAGEMENT ABOARD USS CORINTH (CG-44): A CASE STUDY

12. PERSONAL AUTHOR(S) Gonzalez, Cheryl Louise

13a. TYPE OF REPORT	13b. TIME COVERED	14. DATE OF REPORT (*year, month, day*)	15. PAGE COUNT
Master's Thesis	From To	March 1991	110

16. SUPPLEMENTARY NOTATION
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17. COSATI CODES			18. SUBJECT TERMS (*continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUBGROUP	Information Resource Management, Case Study, Security, Virus, Aegis Cruiser, LAN, Local Area Network

19. ABSTRACT (*continue on reverse if necessary and identify by block number*)

This thesis is a case study that chronicles the information resource management on board an Aegis class cruiser in the U.S. Navy. The events, organization, environment, and personnel involved in the installation and subsequent use of the local area network are documented. Also documented is the "STONED" virus attack on the computers after a light-off assessment of the ship's Engineering plant.

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT	21. ABSTRACT SECURITY CLASSIFICATION	
☒ UNCLASSIFIED/UNLIMITED ☒ SAME AS REPORT ☐ DTIC USERS	Unclassified	
22a. NAME OF RESPONSIBLE INDIVIDUAL William J. Haga	22b. TELEPHONE (*Include Area code*) (408) 646-1276	22c. OFFICE SYMBOL AS/HG

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

Approved for public release; distribution is unlimited.

Information Resource Management
Aboard USS Corinth (CG-44): A Case Study

by

Cheryl L. Gonzalez
Lieutenant Commander, United States Navy
B.A., University of Michigan

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN INFORMATION SYSTEMS

from the

NAVAL POSTGRADUATE SCHOOL
March 1991

ABSTRACT

This thesis is a case study that chronicles the information resource management on board an Aegis class cruiser in the U.S. Navy. The events, organization, environment, and personnel involved in the installation and subsequent use of the local area network are documented. Also documented is the "STONED" virus attack on the computers after a light-off assessment of the ship's Engineering plant.

TABLE OF CONTENTS

I. INTRODUCTION

A. GENERAL DESCRIPTION

This thesis chronicles the events, organization, environment, and personnel involved in the installation and use of a local area network aboard an Aegis class cruiser in the U.S. Navy. Also documented is the Marijuana virus attack on the computers after a light-off assessment of the ship's engineering plant. The information is presented in a case study format that covers a period of two years and is analyzed in light of the rapid evolution and spread of information systems technology.

B. METHODOLOGY

A case study is a description of a real situation that occurred in a real organization (Cohen, 1980, p. 108). A case study evolves from one or more key issues or problems in a given situation. This case will concentrate on the issues faced by shipboard personnel on board an Aegis class cruiser in the U.S. Navy. It will consider information resource management, leadership, planning, technical issues, and security. This case will also focus on the decisions made during the installation of the ship's local area network and those pertaining to the network's current use. A case study is an effective method for presenting valuable

insight into the constant technological change and innovation characteristics of the computer systems management field and their effects on management and organization change (Benbasat, 1987, p. 370).

This thesis is written as a teaching tool and re-creates the ship's environment and portrays its characters so as to present a situation where students discern the problems and recommend solutions. The information is presented in chronological sequence using a narrative and dialogue format. This format is designed to facilitate the probe for questions and answers, problems and solutions. The dialogue will allow the reader to learn about the personalities of the persons making decisions and the users who must perform their assigned duties using the computer tools that result from these decisions. Personalities are often key to understanding how and why certain decisions are made. The name of the ship, ship's personnel, contractor and personnel, and maintenance facility personnel have been changed for purposes of confidentiality.

Information regarding this case comes from written documentation, interviews, and direct observation of everyday practices aboard the ship. Presenting the information in chronological sequence provides a logical discussion of the decisions and events surrounding the installation and use of the local area network. This method

encompasses the depth necessary for the details and processes within the situation to be completely understood.

C. BACKGROUND

The local area network documented in this thesis is on board the USS Corinth (CG-44). The network is currently used for the eight o'clock evening status report of the ship's departmental spaces. The seven Zenith-248 personal computers (one of which is the network server) are also used as stand-alone computers for word processing.

The network was the first to be installed on a combatant ship homeported in San Diego. The network installation was an effort to move the ship toward a "paperless" environment.

D. EDUCATIONAL OBJECTIVES

There is one primary and several secondary items that are of interest in this thesis. The primary objective addresses how the ship's personnel can use the local area network installed on board the ship to meet the administrative requirements of their operational commitments. One secondary objective addresses how the commanding officer can be convinced that the network will enable the ship to become a "paperless" environment. Another secondary objective addresses how the Shipboard Non-tactical Automated Data Processing Program (SNAP) II system relates to the recently installed network. SNAP II was

installed prior to the network in an attempt to alleviate the ship's administrative burdens. The next secondary objective discusses the new standards of architecture that must be installed to offset the incompatibility, if any, between the Zenith-248 and the Desktop III contracted for with UNISYS. Another secondary objective focuses on the issue of security. Security will be investigated to discern what security measures are currently in place, what potential risks, if any, exist, and what security measures, if any, should be taken. The final secondary objective to be addressed concerns the number and location of the computers. How many computers are required and where should they be located in order to maximize the ship's administrative efficiency and effectiveness?

E. ORGANIZATION OF THESIS

Following this introductory chapter, the thesis is organized into six chapters and ten appendices. Chapter II is a discussion of the case methodology regarding its advantages and importance as both a research and teaching strategy. Chapters III, IV, V, and VI are the case study of the local area network on board USS Corinth. Chapter VII is the case analysis of the installation and use of the network. Chapter VIII provides the conclusion and recommendations as they relate to the Educational Objectives

outlined in this chapter. The Appendices pertain to the case, and provide amplifying information.

II. CASE METHODOLOGY

A. INTRODUCTION

This chapter defines case methodology. Other research methods will be compared to the case study method, drawing contrasts and parallels between them. The benefits of a case study in terms of research and teaching will also be discussed.

B. CASE STUDY FOR RESEARCH PURPOSES

The case study stands on its own as a research strategy as evidenced in the following definition:

> A case study is an empirical inquiry that
> - investigates a contemporary phenomenon within its real life context; when
> - the boundaries between phenomenon and context are not clearly evident; and
> - multiple sources of evidence are used. (Yin, 1976, p. 23)

Prior to this definition, a common misconception held by those uneducated in case methodology was that research strategies were of a hierarchical nature (Yin, 1976, p. 15). Historically, case studies were considered to be at the bottom of the research hierarchy. Case studies were often used as the preliminary part of other types of research.

Presently, however, views on conducting research have evolved to the point that each different type of research strategy is seen as "a different way of collecting and

analyzing empirical evidence." (Yin, 1976, p. 15) Today, the research strategy selected is based on the subject matter and research objectives. Research serves one of three purposes: exploration, description, or explanation. Each research strategy can be used for each of the research purposes. The strategy selected depends on the following conditions: (1) type of research question; (2) extent of control over behavioral events; (3) focus on contemporary or historical events (Yin, 1976, p. 16).

There are five research strategies recognized within the social sciences: experiment, survey, archival analysis, history, and case study. Case study, history, and experiments are the only research strategies that will be addressed. They are used to answer the "how" or "why" research question. A case study focuses on contemporary phenomena where there is no control by the researcher over the behavior of the persons involved in the case. History's focus is on past phenomena with no requirement to control behavioral events. The case study research method has the advantage of adding direct observations and interviews when compared to history. This advantage is due primarily to the difference in research focus, present versus past. Experiments, on the other hand, focus on contemporary phenomena and require control over behavior. Traditionally, researchers have emphasized quantitative and controlled events in an effort to generalize the results, as well as,

replicate the event. Today, these researchers recognize the benefits obtained from case research as being more than an analysis of decisions or events. (Yin, 1976, p. 19)

C. ADVANTAGES OF CASE STUDIES

Case studies provide a description of "holistic and meaningful characteristics of such real life events as life cycles, organization and managerial processes, neighborhood change, international relations, and maturation of industries." (Yin, 1976, p. 14) Case study research has a unique strength in its ability to assemble multiple sources of information and present this evidence as a whole, complete picture. It captures a complete understanding of the entire situation, including cause and effect relationships. "As a research endeavor, the case study contributes uniquely to our knowledge of individual, organizational, social, and political phenomena." (Yin, 1976, p. 14)

Qualitative data in the form of words give the case study method another advantage. Qualitative data are a "source of well-grounded, rich descriptions, and explanations of processes occurring in local contexts." (Miles, 1984, p. 15) Personal feelings and opinions, documented through interview and observation, are a vital source of information in understanding decisions made in any given situation. Attitudes, relationships among personnel,

and the power and influence within the organization are portrayed with words. "Words, organized into incidents/stories provide a concrete, vivid, meaningful flavor that often proves far more convincing to a reader...than a page of numbers." (Miles, 1984, p. 15)

D. DISADVANTAGES OF CASE STUDIES

The qualitative advantage found in case study research is also contributing to the difficulty in accepting the case study method as a key research strategy. Words, often having a variety of meanings, are subject to interpretation and could therefore bias the researcher's view of the situation. Also, "observations tend to be unique and non-replicable." (Lee, 1986, p. 2) This suggests that another researcher would not be able to replicate the entire case study from gathering and analyzing the information.

Case study research does not conform to a standard and accepted method of data analysis. This lack of common language contributes to the uncertainty of case study. Case study researchers in the past have been found to influence the case study results.

Several other drawbacks to the case study method are also apparent. Case study preparation is time-consuming and their documentation is voluminous. The fact that there is little basis for scientific generalization is also considered a major stumbling block (Yin, 1976, p. 20). One

who favors the quantitative viewpoint may be skeptical of case study research because there is the tendency to draw generalizations from the conclusions and apply them to other situations. This, however, is not the intent of case study conclusions. "Case study conclusions are generalizable to theoretical propositions and not to populations or universes...In this sense a case study does not represent a 'sample' and the investigators' goal is to expand and generalize theories (analytic generalization) and not to enumerate frequencies (statistical generalization)." (Yin, 1976, p. 21)

The case study as a research strategy has been used in many different areas:

- policy, political science, and public administration research;
- community psychology and sociology;
- organizational and management studies;
- city and regional planning research, such as studies of plans, neighborhoods, or public agencies,... (Yin, 1976, p. 16)

The case study method has proven to be invaluable to the information systems arena. "The information systems area is characterized by constant technological change and innovation." (Benbasat, 1987, p. 370) This technological change and innovation has had a profound impact on management and organizational issues in information systems departments. Case study research has been able to provide

valuable insights into these issues (Benbasat, 1987, p. 370).

E. CASE STUDY FOR TEACHING PURPOSES

In any learning situation there are two factors: the specific knowledge to be learned and the process of learning. The learning process is a method used by the individual to solve a problem or make a decision. A student's knowledge and ability to deal with the reality of life outside the classroom is dependent on both of these criteria. (Pascale, 1973, p. 1)

Case studies present real life situations. Case studies provide a wide range of experiences for the student to compare and contrast. The student may one day find himself in a similar situation and would be able to draw from these case study experiences. "Case studies are valuable lessons in teaching students the habits of diagnosing problems, analyzing, and evaluating alternatives and formulating workable plans of action." (Harvey, 1988, p. 56) Students must also learn that decisions are not made purely from an analysis of the facts. "The decision is a political process...involving power and influence." (Lee, 1986, p. 2)

Using case studies in a safe classroom environment allows the student an opportunity to apply the theory he or she has learned to a given situation. There is also the challenge of testing a theory in a contemporary setting to

prove its validity. If the theory does not hold there is an opportunity to explore the reasons why. Students may debate the issues of cause and effect, problem and solution. These debates will force students to examine their assumptions and defend their positions on the issues. Other benefits of the use of a case study in a classroom include teaching students the following skills: how to search for facts, choose between alternatives, and what questions it is essential to ask. (Pascale, 1973, p. 2)

Retired Navy Admiral Stansfield Turner believes strongly in using case studies within military classrooms. He says, "Many of the education programs, are simply cramming officers' heads with facts rather than helping them to develop the skills to deal with difficult problems of leadership, strategy, and management...the case study method will help prepare students for the time when they rise to the level where they really have to make decisions for our country." (Rosenau, 1988, p. 1)

F. METHODOLOGY OF THESIS CASE STUDY

The case study that is the subject of this thesis chronicles the information resource management of an organization during a two year period. It describes the installation of a local area network in the organization and its subsequent usage. The case also describes the leadership, planning, technical issues, and security as they

relate to information resource management. A case study treats people as the observable agents through which the unobservable forces of the organization act (Lee, 1986, p. 9).

Sources of information included written documentation, interview, and direct observation. Written documentation included publications on software applications, reports written by the contractor about the installation, and articles written on the related computer technology. All interviews but three were conducted in person. The three exceptions were conducted via telephone. Interviews were conducted with personnel from throughout the entire chain of command within the organization, the contractors, and the project managers. The case setting is considered a contemporary situation because computer systems management is a relatively new field.

III. BACKGROUND AND ORGANIZATION

A. INTRODUCTION

CDR Bill Jones, Executive Officer (XO) of USS Corinth (CG-44), stood on the bridge of his ship sipping coffee as he gazed into the auburn hues of another Pacific sunset. Thoughts of his new Captain's ambitions trickled through his mind. When the new skipper, CAPT Joseph Verdi, took command last month, he addressed the crew specifically about his number one priority: to win the Battle E (see Appendix A). Since then every Department Head has realigned his priorities to focus on the Battle E. "Our weapons system is in pretty good shape and should help us win the Battle E," he mused, "but what about our computers?" A year and a half ago a computer network was installed aboard the Corinth. Approximately ten thousand dollars were spent on the network and it is only used for 8:00 reports (the evening status report of a ship's departmental spaces). The Automated Data Processing (ADP) Officer, ENS Greg Smith, had told CDR Jones that the network will not be of much help in winning the Battle E. "The network is configured with some pretty sophisticated machinery," thought Jones, "surely it has the capacity for more than 8:00 reports."

Former director of Surface Warfare, VADM J. Metcalf, USN (Retired), first suggested a "paperless ship" environment in 1986. "Computers have to be the answer to eliminating paper aboard ship," thought Jones. "I wish I knew more about the computing world. There seems to be so much to learn, an entire language of bits, bytes, disks, and display terminals. Where do you begin to catch up to a technology that seems to be moving so fast?"

B. USS CORINTH

The USS Corinth (CG-44) is a Ticonderoga class Aegis cruiser (see Appendix B). She has a gas turbine propulsion plant and, according to JANE'S, FIGHTING SHIPS is the most capable weapons platform in the US inventory for handling the threat of anti-ship missiles. The Aegis cruiser is the leader among ships in shipboard Command, Control, and Communications. These capabilities are, however, degraded close to a land-based airfield and when operating during simultaneous air/surface/sub-surface engagements. Its advantages are: extended range of its sensors, fast reaction time, ability to track several targets at one time, ability to send combat data automatically to other units, and data displays which combine sensor data with other inputs to convey combined information to users. Its long-range radar gives its operators additional time to respond, gather more data, and make better decisions about threats.

C. ORGANIZATION

The USS Corinth (CG-44) has 365 crew members assigned: 35 officers and 330 enlisted personnel. There are four departments: Engineering, Combat Systems, Operations, and Supply. They report to the XO who reports to the Commanding Officer (CO), CAPT Verdi. (see Appendix C) The Administrative (Admin) Division is part of the Operations Department and its Division Officer, ENS Smith, replaced LCDR Wade Whitaker, Supply Officer, in his collateral role as ADP Officer a year ago.

Due to the administrative nature of the XO's duties he has an open door policy for ENS Smith's Admin Division. ENS Smith reports to LCDR Peter Knight, Operations Officer (OPS), regarding division officer and personnel matters such as leave, liberty, disbursing (pay and allowances), enlisted evaluations, officer fitness reports, and training. The deadlines for submitting officer fitness reports (fitreps) and enlisted evaluations (evals) to Navy Military Personnel Command (NMPC) are not being met. NMPC maintains copies of all naval personnel service records which are used in promotion boards. Several floppy disks have been lost on the Corinth in the process of submitting the fitreps and evals. The process of submitting the reports on board the ship requires submitting a floppy and paper copy of the report to the next person in the chain of command.

Other crew members from various departments aboard ship have been assigned collateral ADP or Local Area Network (LAN) duties. ETC (Electronics Technician, Chief Petty Officer (E-7)) Mark Fisher, of the Combat Systems Department, is collaterally assigned as the Network Supervisor who handles user privileges and updates passwords. YN3 (Yeoman Third Class Petty Officer (E-4)) Fred Johnson, Admin Division, is assigned as Assistant Network Supervisor and LTJG Richard Cash is assigned as ADP Security Officer.

Because the ship has so many junior officers, LCDR Whitaker asked to be relieved of the ADP duties shortly after CDR Jones reported aboard. LCDR Whitaker felt the junior officers needed the collateral duty experience for professional development more than he did. LCDR Whitaker had been instrumental in getting the network installed aboard the ship.

He had drafted the message in October 1988 requesting the installation as part of his collateral ADP duties. (see Appendix D) The previous XO, CDR Brian Moore, had sent the message to Commander, Naval Surface Force, U. S. Pacific Fleet (SURFPAC) for approval. It was approved and the network was installed. The previous CO, CAPT Dewey White, was irritated that CDR Moore spent so much time with the computers. Over time, however, the captain got interested in computers himself. He wanted the various ship's logs on

the network instead of in log books. He also wanted the system to provide navigational plots. In addition, the captain had wanted to be able to push a button which would allow him to determine the status of all operational spaces including weapons, engineering, and communication. CAPT White had been considered a micro-manager by his officers and was not well-liked by the ship's crew. His push to have the network used to its full potential by his crew met with resistance and resentment within the wardroom.

LCDR Knight, with a 115 man department, was especially resistent to the network's installation. "I resented being treated like a yeoman and not a manager," he said. "Why should I type everything? What really upset me, though, was when CAPT White wanted instant status reports. Let's face it, a department head does not want the CO to know about a broken piece of equipment before he (department head) does. That would be embarrassing. Every department head wants to fix the broken equipment or at least know the equipment is down and the fixing is in the works before he reports the status to the CO."

LCDR Steven Finley, Combat Systems Officer (CSO), resented the network installation because he disliked computers. "I am afraid of them because I do not know that much about them," he related. "It seems most computers are only used for word processing." He has 15 - 20 users who have very little computer experience and no one to train

them. Training is virtually non-existent aboard the Corinth. "Computer training should start when a person enters the Navy at boot camp or OCS (Officer Candidate School)," said Finley. "There is no time to read, let alone understand, the volumes of technical manuals that are provided with the system. Since I do not know a lot about computers I do not force my people to use them. If I did I would push my people to use them."

GMM1 (Gunner's Mate, Missile First Class Petty Officer (E-6)) Jeremy Andrews, who works for LCDR Finley, talked about training, "I have personally tried four different times to conduct computer classes after working hours. A few people would sign up but then no one showed up. They either forgot or had after hours conflicts. The training needs to be mandatory and conducted during working hours. We should have a PQS (Personnel Qualification Standard) to be Network Supervisor, ADP Security Manager, and user. I set up a PQS training program for computers at my last command and it worked exceptionally well."

CAPT Verdi has focused on attaining the Battle E. He feels he is on par with his contemporaries in terms of computer literacy and in some cases, well ahead of them. The computers do not seem to fit into his game plan as they did in CAPT White's. CAPT Verdi is a quiet man who keeps to himself and lets his officers do their jobs without watching

over their shoulders. The crew seems to work well under the new skipper's leadership.

LCDR Whitaker commented on the current plans for the network, "If this network is going to make a contribution, the new CO is going to have to push it. If the CO gets interested in the network, believe me the wardroom will get interested in a hurry. Then things will begin to happen. If you want anything done on board ship, it has to start at the top."

IV. NETWORK INSTALLATION

Between 14 and 30 November 1988, Integrated Computer Systems, Inc. (ICS) installed a Local Area Network (LAN) for personal computers on board the ship while it was in port. The installation was done as the result of LCDR Whitaker's submission of a work request to Shore Intermediate Maintenance Activity (SIMA), San Diego. This installation was a maverick of sorts as it was the first LAN installed on a combatant. SIMA had previously been installing LANs, in conjunction with ICS, on board tenders and repair ships. SURFPAC, Code N73, had to approve the installation before SIMA could begin the work.

"The XO of the ship was hot to have the network installed," related John Welford, a computer consultant with ICS and former Navy Supply Corps officer. "The XO said he was tired of the "sneaker-net" (running floppies back and forth between departments) and had heard at the club that networks were the way to go. Unfortunately, the XO was not sure what he really wanted, just that he wanted to stop running floppies back and forth from department to department." SURFPAC was hesitant to approve the installation of the LAN, preferring to wait for SNAP III.

SNAP III is currently in the planning phase and is projected to be on-line in the mid 1990's. It is touted as

the "cure-all" for non-tactical data systems. SNAP III will probably be a multi-server network using 386 servers and 386 SX workstations as well as CD/ROM technology. In all likelihood it will be a mouse-driven software environment and will probably be UNIX-based (because of the portability of UNIX). SNAP III appears to be an effort to move ships toward the "paperless" environment.

The XO thought Naval Sea Systems Command (NAVSEA) and Space and Naval Warfare Command (SPAWAR) moved too slowly on computerization. He did not want to wait years for SNAP III; so he pushed hard for SURFPAC approval. The XO also thought SNAP II to be antiquated and feared that SNAP III would fit into that same category. SURFPAC finally approved the installation even though it was the first of its kind. "I guess there are politically sensitive issues with regard to SNAP III that also caused hesitancy on SURFPAC's part," stated Welford, "but, hey, it was approved and we installed the LAN."

Carl Roberts, a computer engineer from ICS who works on-site at SIMA, recalled SURFPAC's hesitancy to approve the LAN installation. "One of the major problems SURFPAC faced in making the LAN installation decision aboard the Corinth was there was no standard to conform to." SURFPAC shop N41, which deals with tenders, repair ships, ship yards, and repair facilities under NAVSEA jurisdiction, and shop N73, which works with the combatants, had to come together and

attempt to standardize LAN installation procedures and practices. SIMA, in conjunction with ICS, developed a standard for LAN installations and submitted it to NAVSEA in May 1990, approximately one-and-a-half years after the LAN installation on board the Corinth. "We are currently working under this standard until told otherwise by the powers to be," said Roberts. "The Corinth LAN was installed prior to this standard." (see Appendix E) The standard calls for the use of fiber optic cables in accordance with OPNAV and SECNAV. The use of fiber optics is the only way to prevent signal interference with the massive amounts of RF radiation found on board ship. "Interestingly," continued Roberts, "the commercial sector does not have that many fiber optic systems available."

The LAN type installed was an IEEE 802.3 10BASE5 ethernet. It was chosen because of its current use by SURFPAC in the Maintenance Resource Management System (MRMS) and the Type-commander's Headquarters Administrative Information System (THAIS) as well as its predominance in the commercial sector. Ethernet is currently the most popular network architecture, according to Susan Frankle, LAN research analyst with International Data Corporation in Framingham, Mass, but token ring will catch up by 1991 or 1992 (Fox, November 1990, p. 19). The installation involved routing 700 feet of coaxial cable, which was primarily a shipboard self-help project, installing ten ethernet

transceivers, and the attachment of seven Zenith Z-248 personal computers with drop cables and ethernet cards to the network (see Appendix F). Novell Netware was chosen for the network operating system because it is widely used within the Navy and it is used on THAIS. ICS is an authorized reseller of Novell software and has several engineers on staff who are Certified Network Engineers (CNE) who can install the software. The network server has a 70Mb hard disk drive. The Z-248 personal computers had previously been purchased through the Navy's supply system. Each has a 20Mb hard disk drive. The cost of the network installation was $9876, which included the Novell software, the 700 feet of ethernet cable, the network boards, and the ten transceivers.

The transceivers were 3COM model 3C107. They provide fast, convenient attachment of computers to an Ethernet 10BASE5 CSMA/CD local area network and they comply with IEEE 802.3 specifications. A transceiver allows devices to be attached without taking down the network. It provides a Signal Quality Error (SQE) test that checks the collision detection circuit and the connection to the attached device. The transceiver has a built-in jabber control to protect the network from errant transmissions from an attached device. (see Appendix G)

There was no direct installation labor charge to the ship as ICS was already under contract to SURFPAC for LAN

installations. The labor was paid for by SURFPAC through the contract. Henry Atkins, an engineer at SIMA, estimated the labor costs. "The contract between SURFPAC and ICS was negotiated by the Naval Regional Contracting Center for the fiscal year," related Atkins, "and the government usually negotiates for a six percent profit for the civilian company." The three full-time employees each worked 80 hours per week for the two week installation period at a cost of $5786 and the one part-time manager at a cost of $2307 for the two-week period. The two week period was ten working days. The engineer who rode the ship for one week was also calculated based on an 80 hour work week and was approximately $1000. The calculations for the three full-time engineers are based on the company's employees earning $25,000 annually and include fringe benefits. The manager contract cost is based on a $50,000 annual salary and fringe benefits.

The ethernet cable installed is of the Plenum type which meets the requirements of the National Electrical Code for installation in an environmental air space because it does not produce toxic smoke when burned.

The installation was completed prior to the ship's deployment in December 1988. One of ICS's computer consultants, Joe Clark, rode the ship to Hawaii enroute to its WESTPAC deployment, to train selected crew members on the network. The following topics were covered as part of

the network supervisor training: the Novell Netware operating system generation, configuration, and installation; the creation, deletion, and modification of directories, groups, and users; how to establish privileges and trustee assignments for groups and users; controlling jobs on the network; performing backups; bringing the server up and down; managing user accounts; troubleshooting the network; and general network maintenance. RMC (Radioman Chief Petty Officer (E-7)) Wilburn was originally trained as network supervisor. He has since transferred and ETC Fisher was assigned as network supervisor. ETC Fisher has not been formally trained as network supervisor.

Minor problems were encountered during the LAN installation. According to ICS, the Operations Department could not be connected to the network because they were short one transceiver. ICS reports the transceiver was ordered but the ship had yet to receive it. This contradicts the crew's perception of the situation. "We have the workstations," related LCDR Knight, "but there was some problem during the installation and the computers were not connected to the system. I guess ENS Smith is in charge of that matter as ADP Officer but he has not done anything to remedy the situation as far as I know. I am not sure he knows what the problem is. Then again, the skipper has other priorities on which to spend the ship's money."

A batch program was installed to prevent recurring problems with the operating system when using applications that changed user directories. The three-line batch file returns the user automatically to his home directory (the directory the user is in when he logs on to the system) when he exits any program, regardless of the drive he is using.

The network server, located in the Career Counselor's office, was required to be mounted on a shock absorbing pad but none was available. Plans were made for SIMA to provide the pad when the ship returned from deployment. Additionally, some of the workstations did not have enough storage space available on their hard drives so it was necessary to omit some application programs from these workstations. The Supply department ordered additional memory boards to upgrade those workstations.

"The network is not set up efficiently," stated GMM1 Andrews, who has been working with computers since 1969 and has almost completed a degree in Computer Science. He is also one of four partners who own an international computer company. "One of the problems," he continued, "is that there are not enough terminals. Someone is always waiting to use a computer. Another problem is that Enable is not network compatible. This is because it has no locking out features. WordPerfect and WordStar will do file locking." When a crew member is entering data on their portion of the 8:00 report, another crew member can log on to the system

and call up the same report and update his portion at the same time. However, only one update will be accepted by the system. Supply department compiles the 8:00 report. One of the departmental personnel always has to go back to get re-update information from the departments because it was not accepted by the system. Andrews is working on a program for the 8:00 report that is system compatible and has a lock out capability. He has been working on it for over a year and is 80 percent complete. He is using dBASE III Plus and Clipper, a dBASE compiler. Andrews lamented, "Our ship's weapons system is so sophisticated, state-of-the-art and yet the rest of the Navy's computing is behind the technology power curve."

The network has had minimal downtime. It has only been down four times in the last year. The first time it was down was for one and a half weeks because ETC Mark Fisher and GMM1 Andrews did not have time to get to the system. The other downtimes were for only two to three days each.

The captain has authorized $6,000 for ADP per year from the ship's OPTAR. This includes everything from purchase of equipment to maintenance to installation fees. However, the money has already been spent, but not on ADP. "Our Aegis equipment now has to be funded out of our OPTAR," explained ENS Smith. "The Navy used to fund Aegis equipment but now the ship is responsible for funding it. Because of this the

CO used the computer money to pay for Aegis equipment and maintenance."

V. APPLICATIONS AND CONTRACTS

A. INTEGRATED COMPUTER SYSTEMS (ICS)

ICS was founded in 1980 and has over 650 employees nationwide. ICS's expertise lies in systems engineering and the technical support they provide to government and commercial developers and users of electronic systems. The services provided cover the entire system life cycle including: design, development, integration, test, operations, maintenance, calibration, and repair.

ICS has provided solutions to meet client requirements on a broad range of technologies - from front-end systems integration to operational support. Once a client's functional requirements are understood, ICS defines a system to meet them. It provides a system that includes hardware, operating system, and application software. Security specialists can conduct threat assessments and evaluate a system's ability to resist security attacks. Engineers install and integrate an optimal system configured to meet user requirements. System performance verification is included as part of the on-site installation.

ICS training specialists provide classes in the operation and maintenance of information systems. ICS personnel are available to operate the user system while

user personnel are being trained. These operational activities include: data entry, running back-ups and printouts, and system configuration management and control. ICS provides preventive and corrective maintenance support for both hardware devices and software programs.

ICS programmers are experienced in many software languages, including: BASIC, C, COBOL, dBASE, FORTRAN, PASCAL, and several Fourth generation languages. Information systems configured by ICS include a wide variety of hardware devices: mainframes, minicomputers, microcomputers, graphics and publications workstations, mass storage devices, output devices, local area networks, bar code readers, communication systems, and emergency power systems. ICS has had a successful decade of systems integration as noted by their numerous awards and commendations for the company and for individual employees as testimony of their astute professionalism.

B. NOVELL

Novell Netware is the network operating system running on most local area networks. Netware arrived on the computing scene about the same time as the IBM PC. The purpose of Netware was to allow microcomputers to share files stored on the server and to share peripherals such as printers. Netware 286 Advanced was installed aboard the USS Corinth. The Advanced Netware allows 100 users to access the

file server simultaneously and permits multiple servers to exist on the same LAN. Advanced Netware has a feature called Hot Fix which protects a user from certain types of disk failure. The Hot Fix feature checks all data after it has been written to the file server disk. If the data written to a particular area of the disk fails this check, then it is rewritten to another part of the disk while the failed area is marked as unusable.

Advanced Netware allows a maximum of 32,000 files per volume (a physical area of disk space assigned a label or name), a maximum of 1,000 files open concurrently, 32 volumes per server, 255M maximum volume size (the volume must be contained on one disk), and requires a minimum of 2M server memory. Advanced Netware is designed to run on PCs with an 80286 or 80386 CPU. Advanced Netware uses directory caching where the hard disk's directory and file allocation table (FAT) are stored in server memory. Directory caching allows the server's CPU to access the hard disk directory and FAT instantly. Advanced Netware also uses *directory hashing* to search for a file on the file server. This process systematically divides the directory into subsequent halves and searches only a subset of the whole for the requested file.

Novell conducts a five day training course on how to manage the network which includes maintenance and troubleshooting. The course costs $1,500 - $1,800 per

person which is almost equivalent to one department's OPTAR for one quarter. For instance, CSO department OPTAR is $2,500 per quarter.

The USS Corinth network offers the following options on its main menu: MAIL, MESSENGER, NOTIFY, CHANGE PASSWORD, CHAT UTILITY, COPY FILES, ENABLE, FILE MANAGEMENT, MICROSOFT WINDOWS, NETWARE UTILITIES, SESSION MANAGEMENT, and SYSTEM HELP. MAIL is simply electronic mail, the ability to send and receive messages from other users on the network. MESSENGER allows the user to send or receive mail without leaving the application he is currently running. NOTIFY allows the user to check any new messages that he has on file without leaving the current application. This feature uses a hot-key sequence, in this case Alt-S. "RMC Wilburn was the resident expert for MESSENGER and NOTIFY, but he has transferred," said YN3 Johnson. The CHAT UTILITY allows a simultaneous two-way conversation between two users on the network, using typing instead of talking. "CHAT is lots of fun," related YN3 Johnson. "Even the XO thinks it is pretty neat, but he doesn't use it that often so I have to keep going up to his stateroom to show him what to do." YN3 Johnson found COPY FILES confusing. When he wants to copy files he goes to DOS because it is easier and quicker for him. DOS is not available on the network system. "I modified my system so I can use DOS," said Johnson. "It is

fun to play with the system and try to figure out how things work. Everything has a back door."

FILE MANAGEMENT shows information about the user's privileges on the system: create, delete, modify, read and write to files, and search for files. Each user has different system rights depending upon their job requirements. The network supervisor and assistant supervisor have maximum privileges. The network supervisor owns the whole system and can access all other user directories and also sets the options available for each user. Hidden files are under the file search attribute. NETWARE UTILITIES include options: **Check Volume Statistics** which provides such information as the number of files and number of directories available; **Enter DOS** which is available only to the network supervisor; **Gripe to Network Manager**; **List Drive Mappings** which can send the user to any listed subdirectory except Enable; **Users on System**; **Memory Management**; **Network Directory** which lists the user's files in the user's subdirectories and when the files were created, last accessed, last updated, number of bytes in the file, file's subdirectories, and user's rights; **Snipes** which is a game that was installed as part of the system; **System Configuration** which provides **Accounting Data**, **File Server Information**, **Group Information**, **Supervisor Option**, and **Default Account Balance/Restrictions**. **Accounting** allows the network supervisor to restrict user time on the system by

defining dates and times the user may log on to the system. **Group Information** provides the subdirectories, name of the department, and personnel with access privileges as part of the group. "A group works on the same principle as the individual user," explained Joe Clark. "Several users may be part of a group and that group has certain access privileges. The users as part of the group will have those access privileges only as part of the group. Their personal user privileges may be quite different." The **Supervisor Option** provides intruder detection and lockout. The network default allows the user five attempts or five minutes to log on to the system. This option gives the supervisor a means to change the default values for tighter security control. The **Default Account Balance/Restrictions** requires passwords to have a minimum length of five characters. It also provides user information on all users who have access privileges to the network. The supervisor can define an expiration date on the user password, after which time the user can no longer access the network with his current password. **Session Management** allows the network supervisor to change the current file server from one machine to another. **System Help** is an on-line manual providing more information about the system and system commands and features. It also contains a glossary and table of contents.

C. ENABLE

Enable is an integrated application program that combines word processing, spreadsheets, databases (DBMS), presentation graphics, and telecommunications, into one program. It also provides a means to move data easily between these modules. Enable is menu-driven but does have the capability of being keyboard command driven. These two methods, however, cannot be used at the same time. The keyboard is generally faster and provides some functions that cannot be used as part of the menu-driven setup. Enable files can be password protected. Enable's advantages versus that of several stand-alone programs are: (1) the purchase price is lower, (2) it is easy to learn, and (3) it allows data integration with its "windows" feature. Enable's disadvantage is that it is less powerful than any single stand-alone application. The stand-alone application provides more features to advanced users and system integrators.

"I use the database module of Enable to keep track of the mailing list for our ship newsletter *Spirit*," said YN3 Fred Johnson. "I also used the database function for the recent change of command ceremony. I even got a NAM (Navy Achievement Medal) out of it." He asked CAPT White what information he wanted to track and what status information he wanted on a regular basis. From his responses Johnson built the database. He had a database of all the guests and

their addresses for both CAPT White and CAPT Verdi. He kept track of whether an invitation was sent, whether they responded, and how they responded (no or yes). And if yes, how many. He was able to tell CAPT White exactly what the captain wanted to know. "I guess that iced the NAM for me," explained Johnson. "The NAM was given to me by CAPT White for the change of command, helping to set up the network, and helping to train people on the network."

D. SNAP II

The constant increase in peace-time administrative requirements, coupled with the reduction of shipboard manning levels, significantly reduces Fleet effectiveness by increasing the administrative burden on the Fleet to an unmanageable level. The original goal of the Shipboard Non-tactical Automated Data Processing Program (SNAP) was to meet Chief of Naval Operation's (CNO) objective number five of 1980: to alleviate "the administrative burden on fleet units." (NAVMASSO Norfolk, March 1981, p. 3) SNAP II also meets the objective required by OPNAVINST 5230.16 regarding fleet non-tactical support, which is "to enhance the readiness of fleet operational and direct support units through the efficient management of ADP resources." (OPNAV Instruction 5230.16, July 10, 1978, p.1) SNAP was designed to provide U. S. Navy fleet units, afloat and ashore, with a standard Automated Information System (AIS) in the areas of

supply, financial accounting, medical, administration, maintenance, and personnel.

The basic philosophy behind SNAP II is to provide a system that is centrally designed, managed, and procured. SNAP II can also be operated and maintained by users who have little knowledge of computers. These principles are an effort to minimize the life-cycle costs of the SNAP system. SNAP II systems are designed to be highly reliable, requiring a minimum amount of maintenance and repair. No additional shipboard personnel are required for the operation and maintenance of the SNAP II system. Personnel with the appropriate technical background such as an Electronics Technician (ET) are trained to operate and maintain the system. Such technicians perform these duties on a basis collateral to their primary duties. SNAP II provides on-line user manuals, documentation, and diagnostic systems in a language that is easily understood by users and system operators. SNAP II computers are designed to run without operators in an unmanned space. Interaction between the user and system is via remote terminals. SNAP II is designed to ensure information is collected only once and to provide maximum automated interface with other fleet or shore automated information systems. Integrated files and records and files are combined in a database, allowing each subsystem to access and use the information in the database and eliminating duplication of data entry. The information

is used to produce documents and reports as required within the activity or external to the activity.

SNAP II systems use Harris series-300 minicomputers and other commercial off-the-shelf peripheral equipment modified for shipboard use. SNAP II is comprised of three primary systems (hardware, software, software applications) joined together under the control of the Harris minicomputer. The hardware and system software are provided under contract with Systems Management American (SMA), Inc. SMA was issued a contract in November 1981 by the Naval Sea System Command "for the acquisition and logistical support of the ADP hardware, software, and related services for SNAP II." (NAVSEA, February 25, 1982) The contract has a 20 year life and is expected to exceed $200 million. The contract was issued to SMA as a Small Business Administration "8-a" contract which is part of a program to "promote equal access to government contracts" for those who are both economically and socially disadvantaged (U.S. Small Business Administration, September 4, 1979, p. 9). The selection process for the hardware was conducted by SMA. Seventeen vendors submitted proposals. In December 1981, SMA announced the selection of the bid by the Harris Corporation. The Harris 300 systems had been selected for SNAP II even though they had never been used in any major business system application.

The application software, the third primary system of SNAP II, is designed, developed, and installed by Navy Management Support Systems Office (NAVMASSO). The applications are written in COBOL but allow users to write and run their own programs in BASIC, MUSE IV word-processing language, or AZ-7 report/query generator language. The application software provided by NAVMASSO cannot be directly interfaced or accessed by user-generated COBOL applications. This prevents the intentional or inadvertent modification of the SNAP II application software and databases.

"This ship does not use SNAP II like my last ship did," stated LCDR Knight about the USS Corinth. "Training records and watchbills can go on the SNAP system, but this ship does not do that."

E. DESKTOP III

Unisys Corporation was awarded the $700 million Desktop III Microcomputer contract on 17 November 1989, approximately one year after the network was installed on board the Corinth. (see Appendix H) The high-powered 32-bit 80386 Unisys machine cannot be used as a network server. Adam Cane, who serves as technical manager on the PC LAN contract and is an official with Naval Regional Data Automation Center (NARDAC) in Norfolk, Virginia, indicated that the contract was designed by the Air Force so the PCs would serve as stand-alone machines or client stations on

local area networks. "There is nothing in the contract that requires these machines to work as a network server," said Cane.

Jennifer Sharp, NARDAC Norfolk's deputy acquisition project manager for Desktop III said the PCs "will not work as file servers for Banyan Vines, Novell, or 3Com Corporation networks, though they work satisfactorily on DCA 10NET." The Navy is working to solve the problem and let the PCs act as host on a local area network. Ms. Sharp indicated that additional firmware and drivers would be required. For the Desktop IIIs to work as servers, a standard interface card with modifications is required. NARDAC Norfolk is close to solving the problem for the Novell Netware at a relatively low cost. Cane said, "The modifications should be included as part of the contract. Of course, that will be up to the Air Force. If the Air Force does not add the modification to the contract all is not lost." The firmware and drivers should be available locally to users who require the modification for the Desktop III to act as a server on a network. If users are willing to wait for a long term solution to the server problem then hardware and software will be available under the PC LAN contract and will include the firmware necessary to modify Desktop III PCs into file servers. That contract will be awarded in December 1990. The delegation of procurement authority for that contract will let it be

modified to include file server support for the Desktop III PCs if such solutions are not proposed by the winning bidder (Brewin, July 16, 1990, p. 6).

A Novell spokesman said his company is working with the Navy to solve the networking problem. A 3Com spokesman said it would be up to Microsoft to help solve the server problem for a 3Com network because 3Com's software runs under Microsoft Corporation's OS/2 operating system.

Another problem encountered by the Navy with the Desktop IIIs is the backlog of orders. There is approximately a three month wait for orders to be filled. Also 90 percent of the Navy's orders were rejected in the first month of the contract. The order forms have been rejected by Unisys because they were filled out improperly. Janice Ricketts, a NARDAC Norfolk computer specialist, said, "The ordering procedures were rather complicated. Most of the problems resulted from the requirement that customers "build" their required configuration on the order form. Desktop III buyers must be extremely specific on their order forms because the factory cannot guess what they want. Also, potential buyers should expect continued delays because a quota system has been imposed on Desktop III, with the Navy quota set at 1,800 PCs per month."

Another problem with Desktop III is that the Enable integrated application system failed its functional test demonstration in February 1990. Major Mark Caper of the

Small Computer Program Office at the Standards Systems Center (SSC), Gunter Air Force Base, Alabama, declined to comment on the remaining problems with Enable.

A Navy source, who asked to have his identity protected, said, "Disgruntled buyers should blame Air Force politics for the problem. Unisys bid what the Air Force asked for. The Air Force does not want the Desktop III PCs to act as file servers because Air Force wants its people to use AT&T 3B2s. They are available under the Small Multiuser Contract. As far as I know, no one is buying 3B2s for anything."

VI. SECURITY DILEMMA

A. "STONED"

"The next step is to get the updated virus scan floppy from SURFPAC," said CDR Jones, addressing his Damage Control Assistant (DCA), LT Bob Wilson, and ENC (Engineman Chief Petty Officer (E-7)) Rob Fielder. "We cannot afford to lose the computers for another two weeks because of a virus. We're going to have to start thinking about computer security on board this ship. The personal computer in USS Corinth's Engineering's Department had recently been infected by the virus known as "STONED". VIRUSCAN Version 3.5V62 (see Appendix I) was obtained by the ship from SURFPAC to identify and kill 88 of the known viruses, including STONED.

At the end of May 1990, MOTRATM EASTPAC (Mobile Training Team, Eastern Pacific) sent one of their training teams to the ship. The training team conducted a light-off assessment of the ship's engineering plant. Basically, the main engines were started as if the ship was getting underway, but the ship remained at the pier. This type of inspection is done after a yard period of 90 - 120 days. The ship had just completed such a yard period. The training team, which specializes in gas turbine plants, used

Engineering's Z-248 computer to type their report of the inspection results. After the training team departed, LT Wilson noticed some problems, "I would sometimes get spurious data when using the word processor for Engineering reports and Enlisted evals." ENC Fielder noticed the same thing, as well as having trouble booting up the computer. As time went on they could not access data on the hard disk or format floppy disks. The computer would respond to access or format attempts with a "bad disk" or "bad sector" error. YN1 (Yeoman First Class Petty Officer (E-6)) Kevin Clark from MOTRATM EASTPAC called LT Wilson to inform the ship that MOTRATM's computers were down due to a virus known as STONED. MOTRATM had contacted SURFPAC who had the same virus. SURFPAC circulated copies of the VIRUSCAN floppy disk to check and kill the viruses (see Appendix J).

LT Wilson noted, "I lost two floppy disks, one of which had most of my working documents. It has taken me days to recover the information I lost and I still haven't replaced it all." ENC Fielder mused, "It seemed like either a timed virus or one that randomly selected its victim, I'm not sure which. It didn't happen every time someone logged on. I do not know that much about viruses. This experience has been an eye-opener for all of us. Unfortunately, some of our personnel, like the LT (Wilson), threw out their disks before we figured out it was a virus."

The network supervisor, ETC Fisher, indicated the virus was self-generating, "It affected the AUTOEXEC.BAT file on the hard drive. The floppies are now screened and each machine has an automatic virus check on it. It can also clean the virus if it's there. It recognizes a number of viruses." (The AUTOEXEC.BAT is a batch file that can be used to set up system defaults each time a computer is booted.)

YN3 Johnson did not believe the virus existed, "There were too many people trying to program the computer to meet their special needs. Every system has a back door. I've changed the main menu to meet my needs. I think they (Engineering) tried to install a CD/ROM and messed up the AUTOEXEC.BAT and CONFIG.SYS files in Engineering and Supply." (CONFIG.SYS file is a list of commands issued to load programs or change system parameters. It is required by the LAN.)

B. VIRUS

The STONED virus characteristics are as follows: the virus remains resident, it infects the floppy diskette boot sector, and it infects the fixed disk partition table. The damage this virus inflicts is that it affects the system run-time operation, it corrupts or overwrites the boot sector, and it directly or indirectly corrupts linkage files.

The VIRUSCAN searches diskettes or hard drives and identifies any pre-existing PC virus infections. It identifies the specific files or system areas that are infected and will also identify the virus strain, displaying the name of the virus and the name of the infected file or system area. The SCAN/D option allows the virus infection to be removed automatically. Should the infection be widespread, the automatic disinfector utilities are available to remove the infected segments of the files. These utilities also repair and restore the infected programs to their original state. VIRUSCAN is able to detect the ten most common viruses which account for over 95 percent of all reported PC infections, according to McAfee Associates.

Computer viruses are killed and removed by the program CLEAN-UP. In most cases, CLEAN-UP repairs the infected files, re-constructs the damaged programs, and returns the system to normal operation. CLEAN-UP will search the entire system for the virus which is to be removed. When the virus is found it is isolated and removed and the infected file identified. If the file is infected with one of the more common viruses then the file can be repaired. If the file is infected with one of the less common viruses, one that cannot be separated from the file, then the infected file is deleted from the disk and system. Before erasing any files CLEAN-UP will display a warning message and there is the

option of overriding the erase function. Removal of the STONED virus can cause the loss of the partition table in systems with non-standard disk controllers or systems that use special purpose device drivers for disk access. A recommended precaution to be taken before removal of the STONED virus is to back-up all critical data. Should the partition table be lost then all the data on the disk will be lost.

C. CONCLUSION

ENC Fielder installed an automatic virus check in the AUTOEXEC.BAT file called VSHIELD. It checks only the boot-up portion of the hard drive but there is an option to instruct the program to scan floppy disks. ENC Fielder formats, checks for viruses, and issues all diskettes to the ship's personnel. He has recently installed the Direct Access 5.0 program in the Engineering spaces which controls accesses to the system. This program also keeps track of the number of accesses, when the system was accessed, who accessed the system, what programs were used, and any unauthorized access attempts. The unauthorized access attempts from a user will only appear after three unsuccessful attempts to log on. "The program has been on the system for one week, said ENC Fielder, "and shows a total of 201 accesses for the week, with most of the accesses using the Enable application program. The system

was used for a total of 35 hours in that one week period. The one week period was Monday through Friday during normal working hours. During that time there were three unauthorized access attempts. Since yesterday, there have been 32 accesses and 12 of 15 working hours were spent on the system." Engineering has also limited the number of users who can access the system. Within the department, only 17 of the 67 personnel assigned to the Department can access the system. ENS Smith states while demonstrating the program in the Admin spaces, "All the computers have the Direct Access program. Oh, I guess that it hasn't been installed on this computer yet. It should be soon."

VII. CASE ANALYSIS

A. INTRODUCTION

This chapter analyzes the case study in the form of a teaching note. The teaching note has three sections. Section One contains questions for the purpose of helping the student prepare for the case analysis or to aid in generating class discussion. Section Two is a summary of the case study. Section Three covers the major issues or problems that appear in the case study. The identification of the issues serve as potential lecture material for the case study when used in a classroom setting. Section Four is the analysis of the case.

B. CASE STUDY TEACHING NOTE

1. Questions

- Can the local area network be used to achieve the commanding officer's goal of attaining the Battle E? If so, how?
- Can the ship be a "paperless" environment? If so, how can it be achieved?
- How does SNAP II relate to the network?
- What problems does the Corinth face with the UNISYS contract for Desktop III?
- Are security measures aboard the ship adequate? If not, why not and what would you do to improve security?

- How do you convince the commanding officer that the network can be used to meet the administrative requirements of the ship's operational commitment?
- Is the network adequate for meeting the ship's requirements?

2. Case Summary

The case study pertains to one of the Navy's newest combatant ships, the Aegis class cruiser. The primary focus is on information resource management. Descriptions of the ship's mission, goals, organization, users, contractor, and installation of the network are discussed. The network operating system is Novell Netware and the word processing application used on board the ship is Enable. Some of the problems encountered during the installation of the network and its subsequent use are also described.

3. Major Issues/Problems

- The network is only used for one report.
- There is no strategic plan for the information resources.
- The attitude toward training is negative and training is not conducted with relationship to the computing resources.
- The installation of the LAN was rushed and user needs and requirements were unknown.
- ADP Officer designation went from LCDR (O-4) to ENS (O-1).

4. Case Analysis

a. "Sneaker-net"

The network has the potential of meeting the ship's administrative demands. The ship has not maximized the potential of this resource. The saga of the evening 8:00 report has proven the network to be ineffective as well as inefficient. The integrated software application, Enable, does not provide a lock-out capability when a file is in use. This means more than one user may be updating the report at the same time. However, only one update will be accepted by the system. Time and energy is wasted when compiling the report because work that has been completed must be repeated. GMM1 Andrews is using dBASE III Plus and Clipper to write a program that will be system compatible and has the lock-out capability. He has been working on the program for one year and is 80 percent complete. Note that there are off-the-shelf word processing software applications available that are network compatible and provide the lock-out feature.

The inefficiency of the network is magnified by the fitrep and eval process. Paper copies of rough drafts and floppy disks continue to be transported via "sneaker-net" from office to office. The network was installed, primarily, to alleviate this scenario. Floppies are often lost which means retyping the document using the paper copy

as a reference. Compounding the problem is the time wasted by personnel who must wait for a computer terminal to complete their tasks.

On the positive side the "sneaker-net" provides decentralized storage while the LAN file server is centralized storage. The centralized storage is more vulnerable than the decentralized storage in the event of a catastrophe, such as the file server going down.

b. Attitude

There is an aura surrounding the network that includes feelings of fear, resentment, complacency, and frustration. Some fear is caused by a lack of knowledge regarding the technological phenomenon known as the computer. Computer technology changes rapidly and many who have not joined the computing bandwagon feel they are being left behind in the dust.

LCDR Finley has clearly voiced his apprehensions regarding his own personal use of the network. Frustration is evidenced by GMM1 Andrews as he views the Navy as being well behind in the information technology revolution. LCDR Knight resented not being treated as a manager and leader with respect to the network. He was resistent to CAPT White's desire of pushing a button and getting a current status report. That is easily understood when some status reports seen first by the commanding officer versus the

responsible department head could have adverse effects on the department head's fitness report. Careers and promotions are governed by fitness reports. Fortunately for LCDR Knight the instantaneous status reports never came to fruition. He also seemed to feel that "real men do not use keyboards."

Another attitude toward the network that surfaces is complacency. This is evidenced by the operations department workstation which is not connected to the LAN, a problem that has existed for two years. Since the commanding officer is not pushing for a solution, ENS Smith has made no attempt to find one. A key to the complacency may lie in the fact that the ADP Officer collateral duty was once at the O-4 level and is currently at the O-1 level. ADP may now be viewed by the remainder of the crew as being of little importance.

The commanding officer has not been convinced that the LAN will be of any value in attaining the Battle E. He feels he is on par with his contemporaries with regard to computer knowledge. CAPT Verdi has not been shown that putting funds or effort into increasing the LAN usage will make the administrative workload more efficient. He is content to maintain the current status quo.

c. Training

Training on the network to increase user understanding of the system and how to make it more productive for the user is non-existent. Initial training of this type was conducted following the installation of the network. There has not been any training like this on the network since that time. There is no interest in after hour training on the part of crew members. There are a few individuals who are interested in maximizing the network's potential. They are known as "hackers" because of their trial and error style of learning the system.

Yet another critical aspect of training lies in the turnover of personnel on the ship. RMC Wilburn was trained by ICS as network supervisor and was considered one of the ship's resident computer experts. He has since transferred, as has his expertise. Typically the turnover of a collateral duty from one member, who is transferring, to another member consists of handing over a notebook with a pat on the back and a wish of good luck.

Training faces another barrier in the form of funding, or more accurately, the lack of funding. The ship's primary mission revolves around the use of its weapons systems. The ship OPTAR must now fund Aegis equipment which takes a large chunk of money out of the budget.

d. Installation

The LAN was installed within a two week period. As indicated by the contractor, CDR Moore, the previous XO, wanted to alleviate the "sneaker-net" means of conducting business. The XO was not specific in stating his requirements prior to the installation. He was in fact pressed for time regarding the installation because the ship was scheduled to deploy for several months. The network training was conducted during the first leg of the deployment voyage. Had time been given to the proper planning of the requirements for the network prior to its installation, subsequent training could have been incorporated into the contract. The contractor, however, readily accepted this challenge because this was the first LAN installation on board a combatant. The installation was successful in terms of setting it up and ensuring all software applications worked as expected.

e. SNAP II Versus LAN

SNAP II is designed to provide a Navy-wide standard for automating the areas of supply, financial accounting, medical, administration, maintenance, and personnel. It is a highly centralized system which could present problems in meeting the variety of specialized needs required by the different classes of ships' missions. SNAP II is viewed by the previous XO, CDR Moore, as being

antiquated. He strongly desired to press forward and get in line with the information technology revolution. There are also members of the crew, such as LCDR Knight, who wonder why SNAP II is not used for training records and watchbills. Part of the desire to use the SNAP II system by LCDR Knight may arise from his familiarity with the system.

f. Desktop III

The Desktop III is an IBM compatible machine and could be connected to the Corinth's network as a workstation but not as a server. Desktop III is viewed as being a superb unit but problems could surface when ordering the computer. The imposition of a quota system on the Navy and the backlog of orders could cause difficulties in obtaining the computer when it is required. Planning and building the required configuration of hardware could restrict the Corinth because of the lack of resident expertise in this area aboard the ship. The integrated software application, Enable, has failed its functional test demonstration. This may require the ship to purchase a different software application should it need Desktop III computers in the future.

g. Security

The security weaknesses on board Corinth are evidenced by the "STONED" virus. Security training is not scheduled and a contingency plan for security does not

exist. Ignorance is prevalent regarding security practices and viruses. Security has functioned on the ship as an afterthought rather than being part of the initial planning for the network.

VIII. CONCLUSIONS AND RECOMMENDATIONS

A. CONCLUSIONS

1. Rapid Technological Change

Computing devices have existed for thousands of years. The abacus of ancient Greek and Roman civilizations may well have been the first computing device. The gear driven mechanical machines of Blaise Pascal (1623-1662) and Wilhelm Leibniz (1646-1716) were followed some time later by Charles Babbage's (1792-1871) computing device, which was designed to communicate the sequence of steps to perform its task via holes in paper cards. Then came Joseph Jacquard's algorithmic loom of 1801 followed more than a century later by the electromechanical computing devices of Bell Laboratories and Howard Aiken in the mid 1940's. Technology has advanced from the development of the first fully electronic computer which was based on the use of vacuum tubes, then through the use of transistors, to today's use of integrated circuits.

The microprocessor revolution began in the early 1970's. Computers are becoming smaller, yet faster, more powerful, and even cheaper. The ENIAC (Electronic Numerical Integrator And Calculator) was large and expensive, occupying more than 1,800 square feet of space and costing

almost $800,000 (approximately $8 million in 1989 dollars). By comparison today's laptop computer is small, weighing roughly 14 pounds and relatively inexpensive, costing $2,000 to $4,000 depending on user needs or desires.

For centuries computing devices slowly evolved into smaller, faster, and more sophisticated devices. Now the technology is moving so rapidly that the computer purchased today could possibly be obsolete tomorrow. Information technology with high-speed computers has indeed had a very short life. Over a 10^6 improvement in processing and storage capacity has occurred since 1953, and the rate of change is expected to continue at the same pace at least through the 1980's and early 1990's (Cash, 1988, p. 4).

Information technology exploded into such complexity in 1973 that specialized departments within organizations have been created to get the job done. This evolution of computing technology also created diverse challenges for senior members in the military organizational structure. Most of these members received their education and early work experience prior to or during the start of the information technology revolution that began in 1973. The apprehension on the part of senior ranking officers on board USS Corinth toward the 'modern' computer network is, therefore, justifiable.

The Navy is just beginning to taste the essence of the information technology revolution. Officers such as

CAPT Verdi and LCDR Finley entered the Navy just prior to and during the start of this contemporary phenomenon. They have difficulty in comprehending and assimilating the changes in computer technology and applying it to a method of getting the job done more effectively and efficiently. The inefficiencies of the evening 8:00 status report, missed deadlines on fitreps and evals, and personnel waiting to use the computers are accepted.

Budget constraints also add to the problem of keeping up with the technology. For instance, there is off-the-shelf software available that will provide the lock-out feature required for the 8:00 report. It is unfeasible to purchase this software when the funds are not available. The ship's weapons system has top priority for funds because it involves the main mission of the ship.

In spite of the technological advances in computing, the ship's crew is having difficulty comprehending and assimilating these changes. This is compounded by the lack of financial resources to keep up with every significant technological improvement.

2. Training

The Navy places an extraordinary emphasis on education. There is a fine line between education and training. Education is a process of teaching one how to think and training is the resultant action of that process.

Education is an important commodity in the Navy. The Navy has correspondence courses, a variety of Navy Campus educational programs, commissioning opportunities for enlisted personnel through education, the Naval Academy, the ROTC program, OCS, and Naval Postgraduate School. PQS is on-the-job training and completion of specific qualifications is required for advancement of enlisted personnel. General Military Training (GMT) provides non-technical training to help Navy personnel fulfill their oath of service and keep them informed on matters regarding their morale.

Training scheduled after normal working hours, while the ship is in port, had empty classrooms. Training must be scheduled as part of the normal work day. The computer training should be individualized, if possible, but no larger than groups of two to three persons. The training should be planned and taught in small blocks of time such as 30 minutes to be effective.

3. **"Paperless" Ship**

The "paperless" ship concept was initiated in 1986 by VADM J. Metcalf when he was Deputy Chief of Naval Operations for Surface Warfare. Project management responsibility was assigned to SPAWAR. The initiative was intended to reduce the requirements for paper-based

technical, reference, and mission critical documents aboard naval vessels.

On an Aegis class cruiser, paper and associated containers weigh 35.9 tons. Approximately 40 percent of the weight is above the main deck. A study completed in May 1987 suggested the best storage technologies: CD/ROM technology for wide distribution documents (i.e., blank forms, general reference/technical manuals, Navy-wide instructions, catalogs, etc.); WORM (write once-read many) for general working documents (i.e., engineer logs, local correspondence, and message files); and magnetic tape for general data files (i.e., inventory records, schedules, ship maintenance plan, financial files, etc.) (Ruff, July 1988, p. 158). The Corinth has a CD/ROM but has yet to install the device. Lack of expertise or use of the wrong expertise may be creating difficulties with the installation of the CD/ROM.

4. Security

Computer technology has facilitated new ways to use, correlate, and manipulate information. High-speed, high capacity computers enable users to search large numbers of records, instantly retrieve information, and link records through computer networks. This has resulted in an enormous increase in the exchange of information and the numbers of

individuals having access to it. Therefore, there are increased opportunities for inappropriate and unauthorized use of sensitive information. Weaknesses in computer security pose a significant risk to the integrity of computer systems and to the sensitive information in an organization.

Computer viruses are spreading at an alarming rate and are security's nemesis. Viruses have existed for decades, started by programmers who wanted to test their creativity. They often pitted their skills against one another in a variety of games. Today there are a growing number of programmers developing harmful viruses and spreading them. There is cause for concern regarding the spread of viruses because of the large volumes of information that are transported via communication networks using phone lines and satellites. This large volume of traffic increases the chances of an organization's network being infected by a virus. There are millions of individuals using computers in the work environment and purchasing computers for home use. Downloading programs from public bulletin boards, sharing software among friends, and taking the floppy disk home from work to complete unfinished business also increases the chance of computer viral infections and their spread.

The best defense against computer intrusion is prevention: a good security system. The main focus when acquiring computers is on the cost, access speed, memory

capacity, type and format of the information to be provided, and the accuracy of the information. There is a tendency to make security an afterthought as it slows down processing speed, requires more memory capacity, and usually makes operations more complicated and expensive.

Several measures may be taken to provide for adequate computer security within any organization. The following is a foundation for an effective information security program: plan for security, protect critical computing resources, and promote good security practices.

B. RECOMMENDATIONS

In accordance with the problems encountered by the Corinth regarding the LAN, the following recommendations are suggested to improve the LAN's effectiveness and efficiency:

- Implement a matrix structure where an ADP team, much like a project team, crosses the functional boundaries of each department. The team leader must be an O-3 or higher to ensure respectability within the organization for information resource management. The team leader must also have the drive and enthusiasm to maintain the team's desired effectiveness. The ADP team will be responsible for ensuring the network is used effectively, developing contingency plans, training, and maintenance (to include upgrades). They will be required to establish security policy, with the commanding officer's approval, to include restricting access where appropriate, security awareness training, and measures to enforce policy.

- Use the contract SURFPAC has established with ICS and obtain their services to train the ADP team as well as users of the LAN. The training should be progressive and enable the crew to use the network more efficiently.

- Enlist the services of ICS to install CD/ROM.
- Adhere to the security practices established in the following checklist:
  - Provide comprehensive security policies for all types of computing and review them regularly to keep current.
  - Identify and safeguard critical computing resources which require the highest level of protection.
  - Conduct an assessment of security risks.
  - Assign responsibilities for security.
  - Address viruses in contingency plans.
  - Protect information about personnel that is stored on the computer hard drive or floppy disks.
  - Restrict the use of software applications on the ship's computers by having the ADP team leader approve all software application installations.
  - Develop a plan of action in the event of a suspected virus attack.
  - Back-up critical data and software for recovery from a virus attack, loss of power, or other computer failure.
  - Promote good security practices.
  - Educate and train personnel with regard to policies, good security practices (such as frequent changing of passwords), and recognition of and response to possible virus attacks.
  - Promote high ethical standards, such as not copying software. Leadership must set the example on this issue.
  - Enforce security policies with appropriate disciplinary action where necessary.
- Develop plans for training and future system changes as they relate to set goals and future personnel turnovers. The plans must be reviewed and revised on a regular basis. The plans must be used

to schedule the training and budget for the system changes.

- The ADP team must thoroughly investigate the most beneficial uses of SNAP II and the LAN.

- The ADP team must thoroughly investigate the Desktop III compatibilities and incompatibilities.

- Gather data using the Direct Access program to determine the number of users, which terminals are used, and when the specific terminals are used. Also, determine the length of time personnel must wait to use a specific terminal. Analyze the data to see which resources could be used more effectively and if more terminals are required.

- Obtain and install the transceiver in the Operations Department. Connect the OPS terminal to the network.

The Navy, DOD, and the government must take a long, hard look at how the private sector is coping with the information technology revolution. These coping methods, however, must be applied with care so the mission of the organization is always given top priority. The various missions of ships and shore activities must also be considered when planning to upgrade information resources within the Navy. The most recent evidence of current technology being successfully used was depicted during the Gulf War. The United States Armed Forces have certainly shown the significance of being on the leading edge of technology.

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF OF NAVAL OPERATIONS
WASHINGTON, DC 20350-2000

IN REPLY REFER TO
OPNAVINST 3590.4G
OP-642C2

4 MAY 1990

OPNAV INSTRUCTION 3590.4G

From: Chief of Naval Operations

Subj: AWARDS FOR INTRATYPE BATTLE EFFICIENCY COMPETITION AND INSIGNIA TO DENOTE EXCELLENCE IN CERTAIN WEAPONS AND OPERATIONS

1. Purpose. To revise rules for the award of ship and aircraft insignia to denote winners of intratype battle efficiency competition or attainment of a high standard of proficiency in certain weapons and operations.

2. Cancellation. OPNAVINST 3590.4F.

3. Discussion. The continuation of the intratype battle efficiency competition is reaffirmed. The Fleet Commanders in Chief under Chief of Naval Operations guidance are responsible for battle efficiency competition policy within their respective fleets.

4. Awards for Intratype Competition. Fleet Commanders in Chief may authorize the display of the following awards and insignia by ships standing first in their respective competitive groups in the intratype competition, and by aircraft squadrons meeting standards set forth in FXP 2 (series) (insofar as practicable; competitive grouping should avoid combining ships or aircraft squadrons assigned basically different missions):

a. The Battle Efficiency Pennant, will be flown per para 1608 of NTP 13(B) (Flags, Pennants, and Customs), from the date the winners of the competition are announced to the date that winners are announced for the succeeding evaluation period. The winners of five consecutive awards are authorized to display a pennant containing a gold ball on a blue field for a similar period.

b. A white "E" on the bridge bulwark (or sail of submarines), from the date the winners of the competition are announced to the date that winners are announced for the succeeding competitive cycle. A service stripe under the "E" for the second and each subsequent consecutive award. A gold "E" in lieu of the white "E" and service stripes, for winning the award five consecutive times. A gold service stripe under the gold "E" for the sixth and each subsequent consecutive award. At the

discretion of the Fleet Commander in Chief, a period during which a ship spends a majority of its time in an overhaul or repair facility may be disregarded in determination of qualification for the above "five consecutive evaluation periods".

c. A plaque, for permanent display, located so that it constitutes display for personnel on board the ship rather than for persons outside the ship.

5. **Insignia to Denote Attainment of Excellence in Certain Weapons and Operations.** Fleet Commanders in Chief may authorize the display of the following insignia to denote attainment of departmental or mission area excellence, based on criteria of day-to-day performance, satisfactory accomplishment of required exercise or their operational equivalent, and satisfactory completion of an operational readiness inspection.

WEAPONS/OPERATIONS	SHIPS INSIGNIA
Electronics Warfare	White "EW"
Gun Firing Systems	White "E"
Surface-to-Air Missile Systems	White "E"
Antisubmarine Weapons and Operations	White "A"
Weapons Department in CV's	Black "W"
Engineering	Red "E"
Damage Control	Red "DC"
CIC	Green "E"
Communications	Green "C"
Minesweeping	White "M"
Assault Boat Operations	Assault Boat Insignia
Air Department	Yellow "E"
Supply Department	Blue "E"
Aircraft Intermediate Maintenance Department	Black "E"
Deck Seamanship	Deck Seamanship Insignia

6. **Period of Display.** The insignia listed in paragraph 5 will be displayed for periods specified by the Fleet Commander in Chief. Service stripes under the insignia indicate the second and subsequent consecutive awards.

7. **Specification for Insignia.** Size, location, and painting specifications for the above insignia will follow Chapter 9190, Naval Ships Technical Manual.

8. **Navy "E" Ribbon.** Wearing of the Navy "E" ribbon by personnel attached to ships and aircraft squadrons designated by the Fleet

Commander in Chief to receive the intratype proficiency award outlined in paragraph 4 is authorized, subject to the provisions outlined in the Navy and Marine Corps Awards Manual (SECNAVINST 1650.1E).

9. Policy Guidance

a. No aspect of the battle efficiency competition should result in impairment of combat readiness. The selection process should, in fact, emphasize selection of those units who have operationally displayed excellence in their warfare missions.

b. The Fleet Commanders in Chief have full authority to modify and discontinue any part of the battle efficiency competition called for by the FXPs.

c. Fleet Commanders in Chief are encouraged to conduct such competition as they consider necessary to strengthen and evaluate unit and force readiness.

d. As directed by the Fleet Commanders in Chief, the Type Commanders will establish criteria for the competition of Naval Reserve Force ships, closely paralleling those standards used for active force ships.

e. As directed by the Fleet Commanders in Chief, the Type Commanders, in conjunction with the Commander, Naval Air Reserve Force, will establish criteria for the competition of Naval Air Reserve units, closely paralleling those standards used for active force air units.

f. As directed by the Fleet Commanders in Chief, the Type Commanders, in conjunction with the Commander, Military Sealift Command, will establish criteria for the Departmental "E" competition for embarked Military Communications and Supply Detachments, closely paralleling those standards used for active force ships.

A. J. KELLY

DEPUTY CHIEF OF NAVAL OPERATIONS
(PLANS, POLICY AND OPERATIONS)

Distribution:
SNDL A5 (Bureaus)
21A (Fleet Commanders in Chief)
22A (Fleet Commanders)
23A (Naval Force Commanders)

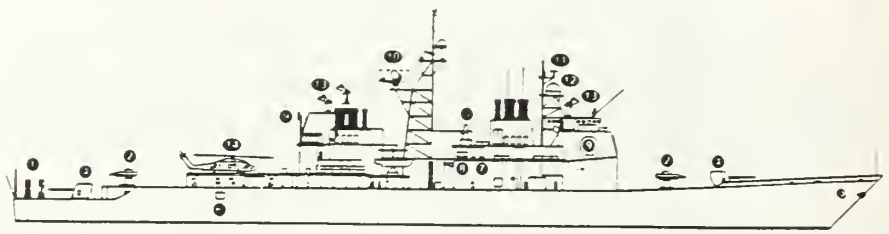
Distribution (continued):

SNDL	23B	(Special Force Commanders) (COMIDEASTFOR, AND USCOMSOLANT, only)
	24	(Type Commanders)
	26	(Special Commands, Groups and Units)
	28	(Squadron, Division and Group Commanders - Ships)
	29	(Warships)
	30	(Mine Warfare Ships)
	31	(Amphibious Warfare Ships)
	32	(Auxiliary Ships)
	41A	(Commander MSC)
	41B	(Area Commanders, MSC) (COMSCLANT and COMSCPAC, Military Departments, only)
	41J	(Military Sealift Command)
	42	(Naval Aviation)
	46	(Fleet Marine Force - Aviation)
	C25A	(OPNAV Support Activity Detachment) (Ft. Ritchie, only)
	FF1	(Naval District Washington DC)
	FKA1	(Systems Commands)
	FL1	(Data Automation Command) (Code 813, only) (25)

OPs 01, 02, 03, 04, 05, 06, 642 (25), 09B and 008

Stocked:
CO, NAVPUBFORMCEN
5801 Tabor Avenue
Philadelphia, PA 19120-5099 (100 copies)

APPENDIX B



TICONDEROGA

(Scale 1 : 1 500)

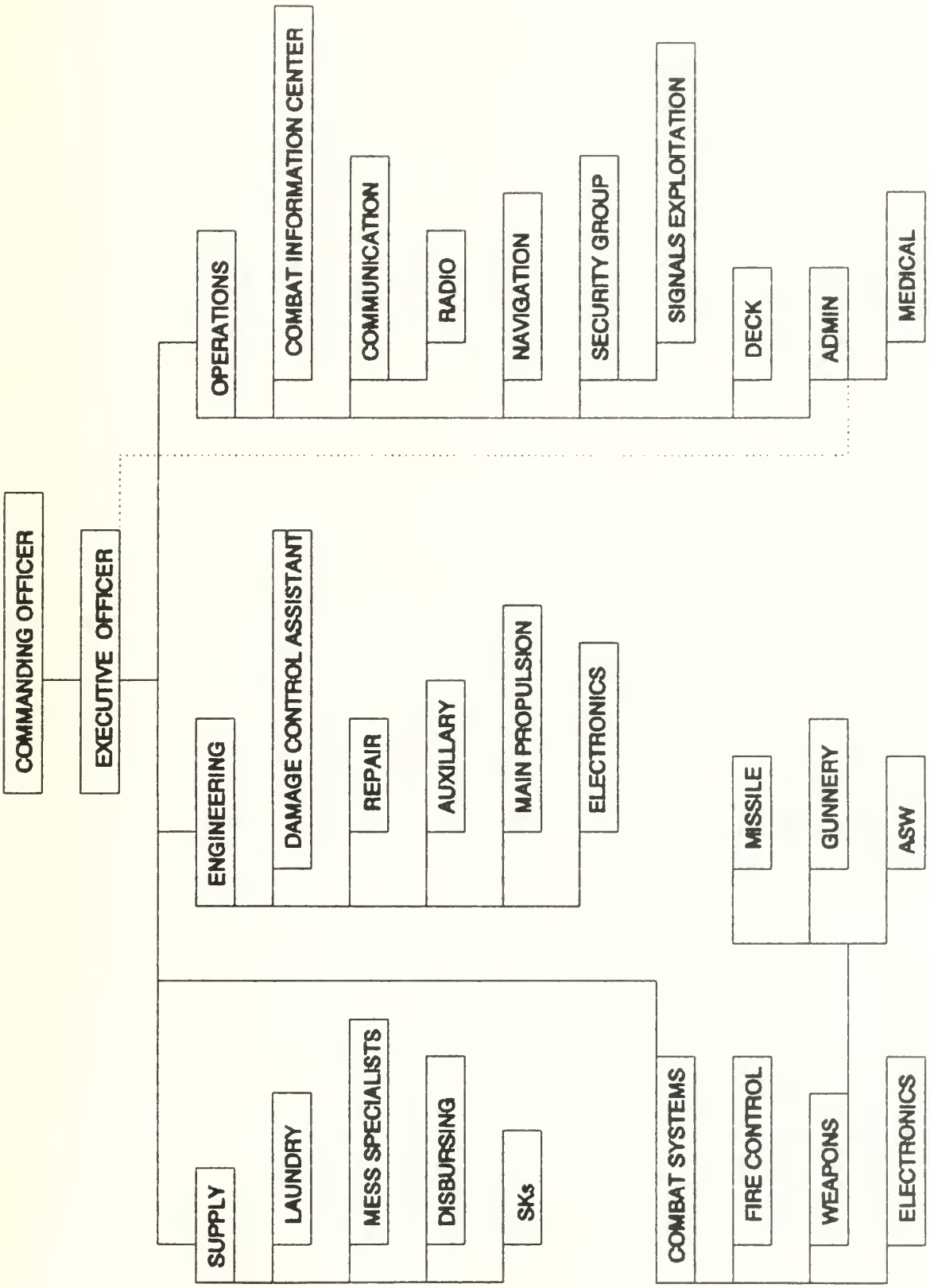
Displacement, tons: 7015 light, 9590 (CG 47-48); 9407 (CG 49-51), 9466 (remainder) full load
Dimensions, feet (metres): 567 × 55 × 31 (sonar) *(172.8 × 16.8 × 9.5)*
Main machinery: 4 General Electric LM 2500 gas turbines, 80 000 hp, 2 shafts
Speed, knots: 30+ **Range, miles:** 6000 at 20 kts
Complement: 358 (24 officers), accommodation for 409

Missiles: SLCM/SSM GDC Tomahawk (CG 52 onwards), combination of (a) land attack, TAINS (Tercom aided navigation system) to 2500 km *(1400 nm)* at 0.7 Mach, altitude 15-100 m *(49.2-328.1 ft)*; warhead nuclear 200 kT (TLAM-N), CEP 80 m, or warhead 454 kg (TLAM-C) or submunitions (TLAM-D), range 1300 km *(700 nm)*; CEP 10 m
(b) anti-ship (TASM), inertial guidance active radar and anti-radiation homing to 460 km *(250 nm)* at 0.7 Mach, warhead 454 kg
8 McDonnell Douglas Harpoon (2 quad) ❾, active radar homing to 130 km *(70 nm)* at 0.9 Mach; warhead 227 kg
SAM: 68 (CG 47-51); 122 (CG 52 onwards) GDC Pomona Standard SM-2MR, command/inertial guidance, semi-active radar homing to 73 km *(40 nm)* at 2 Mach.
A/S 20 Honeywell ASROC, inertial guidance to 1.6-10 km *(1-5.4 nm)*, payload Mk 46 Mod 5 Neartip/Mk 50
SAM and A/S missiles are fired from 2 twin Mk 26 Mod 5 launchers ❷ (CG 47-51) and 2 Mk 41 Mod 0 vertical launchers ❶ (61 missiles per launcher) (CG 52 onwards). Tomahawk is carried in CG 52 onwards with 8 missiles in each VLS launcher and 12 in the magazines. Operational evaluation of VLS continues in conjunction with operational evaluation of Tomahawk. Vertical launch ASROC will be back fitted when available.
Guns: 2 FMC 5 in *(127 mm)*/54 Mk 45 (Mod 0 (CG 47-50); Mod 1 (CG 51 onwards)) ❸, 65° elevation, 20 rounds/minute to 23 km *(12.6 nm)* anti-surface, 15 km *(8.2 nm)* anti-aircraft, weight of shell 32 kg
2 General Electric/General Dynamics 20 mm/76 Vulcan Phalanx 6-barrelled Mk 15 ❹, 3000 rounds/minute combined to 1.5 km.
4—12.7 mm MGs

Torpedoes: 6—324 mm Mk 32 (2 triple) tubes (fitted in the ship's side aft) ❺. 36 Honeywell Mk 46 Mod 5, anti-submarine, active/passive homing to 11 km *(5.9 nm)* at 40 kts; warhead 44 kg. To be replaced by Mk 50 in due course.
Countermeasures: Decoys: 4 Loral Hycor SRBOC 6-barrelled fixed Mk 36 ❻, IR flares and Chaff to 4 km *(2.2 nm)*. SLQ-25 Nixie, towed torpedo decoy
ESM/ECM: SLQ 32V(3) ❼, combined radar warning, jammer and deception system.
Combat data systems: NTDS with Links 4A, 11, 14 and 16 in due course. SATCOM SRR-1, WSC-3 (UHF). UYK 7 and 20 computers (CG 47-58); UYK 43/44 (CG 59 onwards). SQQ 28 helo data link.
Fire control: SWG-3 Tomahawk WCS. SWG-1A Harpoon LCS. Aegis Mk 7 multi-target tracking with Mk 99 MFCS (includes 4 Mk 80 illuminator directors); has at least 12 channels of fire. Mk 116 Mod 7 FCS for ASW. Mk 86 Mod 9 GFCS.
Radars: Air search/fire control: RCA SPY 1A phased arrays ❽, 3D, E/F band (CG 47-58).
RCA SPY 1B phased arrays, 3D, E/F band (CG 59 on).
Air search: Raytheon SPS 49(V)7 ❿, C/D band, range 457 km *(250 nm)*
Surface search: ISC Cardion SPS 55 ⓫, I/J band.
Navigation: Marconi LN 66 (CG 47-48), I band.
Raytheon SPS 64 (remainder); I band.
Fire control: Lockheed SPQ 9A ⓬, I/J band, range 37 km *(20 nm)*.
Four Raytheon/RCA SPG 62 ⓭, I/J band.
Tacan: URN 25. IFF Mk XII AIMS UPX-29.
Sonars: General Electric/Hughes SQS 53A/8 (CG 47-55); bow-mounted, active search and attack, medium frequency.
Gould SQR 19 (CG 54-55); passive towed array (TACTAS).
Gould/Raytheon SQQ 89(V)3 (CG 56 onwards), combines hull-mounted active SQS 53B (CG 56-67) or SQS 53C (CG 68-73) and passive towed array SQR 19.
SQQ 28 (CG 54 onwards); helicopter data link.

Helicopters: 2 SH-60B Seahawk LAMPS III ⓮. 2 SH-2F LAMPS I (CG 47-48).

Jane's Fighting Ship's 1990-91, 93rd ed., p. 742, Jane's Information Group Limited, Sentinel House, 163 Brighton Road, Coulsdon, Surrey, CR5 2NH, UK, 1990.


COMMANDING OFFICER
EXECUTIVE OFFICER
OPERATIONS
COMBAT INFORMATION CENTER
COMMUNICATION
RADIO
NAVIGATION
SECURITY GROUP
SIGNALS EXPLOITATION
DECK
ADMIN
MEDICAL
ENGINEERING
DAMAGE CONTROL ASSISTANT
REPAIR
AUXILLARY
MAIN PROPULSION
ELECTRONICS
SUPPLY
LAUNDRY
MESS SPECIALISTS
DISBURSING
SKs
COMBAT SYSTEMS
FIRE CONTROL
WEAPONS
ELECTRONICS
MISSILE
GUNNERY
ASW

R 241555Z OCT 88
FM USS CORINTH
TO COMNAVSURFPAC SAN DIEGO CA
INFO COMCRUDESGRU THREE
BT
UNCLAS//N05230//
SUBJ: ACQUISITION OF AUTOMATED INFORMATION SYSTEM
A. COMNAVSURFPACINST 5230.1B
1. ZENITH 248 PERSONAL COMPUTERS HAVE BEEN INSTALLED IN EACH MAJOR DEPARTMENT WITH A MULTIFACETED SOFTWARE PACKAGE WHICH HAS STANDARDIZED WORD PROCESSING SOFTWARE ONBOARD SHIP AS WELL AS PROVIDED A PAPERLESS ENVIRONMENT FOR BOTH OFF-SHIP AND INTERDEPARTMENT CORRESPONDENCE.
2. TO TAKE FURTHER ADVANTAGE OF THE TECHNOLOGY AVAILABLE IT IS DESIRED TO INSTALL A LOCAL AREA NETWORK (LAN) WHICH WILL ALLOW SHARING OF FILES AND ELECTRONIC TRANSFER OF FILES BETWEEN WORKSTATIONS.
3. SIMA SD ADP REPS HAVE CONDUCTED A WALK-THRU OF SPACES AND PROVIDED DETAILED RECOMMENDATIONS FOR HARDWARE/SOFTWARE PROCUREMENT. SIMA ADP HAS CAPABILITY AND HAS INDICATED AN EAGERNESS TO ASSIST BY ACCOMPLISHING INSTALLATION. LAN INSTALL WILL NOT REQUIRE VIOLATION OF WATERTIGHT INTEGRITY AND EXISTING CABLE RUNS WILL SUPPORT.
4. IAW REF A, FOL ABBREVIATED SYSTEM DECISION PAPER IS SUBMITTED:
   UIC: 77777
   MAJOR CLAIMANT: CINCPACFLT
   POINT OF CONTACT: LCDR WADE WHITAKER AUTOVON: 958-3333
   1. NEED: ZENITH 248 MICROCOMPUTERS ARE CURRENTLY INSTALLED IN ALL MAJOR DEPARTMENTS AND ADMINISTRATIVE OFFICES ONBOARD BATTLE OF THE BULGE. ADMINISTRATIVE CORRESPONDENCE (LETTERS, MESSAGES, FITREPS, EVALUATIONS, ETC.) IS PREPARED USING ENABLE SOFTWARE AND A PRINTED COPY WITH FLOPPY DISKETTE IS ROUTED/EDITED AT EACH LEVEL OF THE CHAIN OF COMMAND TO SHIP'S OFFICE FOR SMOOTHING. INSTALLATION OF A LOCAL AREA NETWORK (LAN) WOULD PROVIDE CAPABILITY TO PASS FILES ELECTRONICALLY ELIMINATING MULTIPLE HANDLING AND ROUTING OF DISKETTES.
   2. PROPOSED SOLUTION: PURCHASE HARDWARE AND SOFTWARE REQUIRED TO INSTALL LAN WITH DROPS IN ALL MAJOR DEPARTMENTAL SPACES, ADMINISTRATIVE AND EXECUTIVE OFFICES. SIMA ADP HAS PERFORMED A WALK-THRU OF THE PROPOSED SPACES AFFECTED AND RECOMMENDED AN ETHERNET-BASED LAN UTILIZING NOVELL SOFTWARE PACKAGE.
      A. MILESTONES:

	MILESTONE	DATE
(1)	SIMA ADP PERFORM WALK-THRU AND PROVIDE RECOMMENDED HARDWARE/ SOFTWARE REQUIREMENTS.	COMPLETE

(2) DEVELOP ASDP COMPLETE
(3) ASDP APPROVAL 28 OCT 88
(4) ORDER HARDWARE/SOFTWARE 01 NOV 88
(5) SUBMIT AWR REQUESTING SIMA ACCOMPLISH INSTALLATION. 01 NOV 88
(6) RECEIVE HARDWARE/SOFTWARE 14 NOV 88
(7) ACCOMPLISH INSTALLATION 16 NOV 88

3. OTHER ALTERNATIVES CONSIDERED: NONE.
4. COST AND BENEFITS:
   A. COSTS:

NOVELL SOFTWARE	1 EA	$2,021.00
ETHERNET CABLE	1000 FT	$3,500.00
COMMUNICATION BOARDS	7 EA	$2,730.00
TRANSCEIVERS	7 EA	$1,750.00

   B. BENEFITS: PRIMARY BENEFITS WILL BE INCREASED PRODUCTIVITY AT ALL LEVELS OF MANAGEMENT DUE TO THE EASE IN PREPARATION, REVISION, AND PASSING OF DOCUMENTS THROUGH THE CHAIN OF COMMAND USING THE LAN. WOULD ALSO REDUCE MAN-HOURS REQUIRED TO TRACK ADMINISTRATIVE DOCUMENTS AND ELIMINATE COST OF CONSUMABLES REQUIRED TO SUPPORT CONTINUED ROUTING OF DOCUMENTS USING DISKETTES AND HARD COPIES.
5. INTERFACE CONSIDERATIONS: NONE.
6. FUNDING: UNFUNDED IN CURRENT OPTAR. IF APPROVED WILL REQUIRE AUGMENT/ADVANCE.
7. OTHER COMMENTS: NONE.

BT

STANDARD CONFIGURATION REQUIREMENTS FOR THE INTERMEDIATE MAINTENANCE ACTIVITY ADMINISTRATIVE LOCAL AREA NETWORKS

MAY 1990

TABLE OF CONTENTS

1.0 SCOPE

The objective of this document is to define the approved minimum standard for hardware and systems software required for the installation of Local Area Networks to support Intermediate Maintenance Activities under the NAVSEA PMS-331 program. The intent of this document is to provide a basis for compatibility among LAN installations to ensure maximum connectivity.

This standard presents the general minimum acceptable hardware configuration for all phases of Network installation from the network file server device to and including the end user hardware devices connected at each node. In addition, a standard set of system software is prescribed for the Network File Server Devices.

Specific minimum requirements for Intermediate Maintenance Activity PC-LANs to support administrative requirements of the repair departments are also delineated in this document.

2.0 DEFINITIONS

backbone	Major transmission path for a network, usually handling high-volume, high-density traffic.
bridge	Equipment that provides interconnection between two networks using the same protocol structure. Bridges function at the data link layer of the Open Systems Interconnection (OSI) model.
file server	Device (usually a personal computer) that allows users to share files; often enforces network administrator-defined rules for access, permitting reading, duplication, or modification to authorized users.
Gateway	The hardware and software necessary to make two technologically different networks communicate with one another. Porvides protocol conversion from one network architecture to another and may use all seven layers of the ISO/OSI reference model.
IEEE	Institute of Electrical and Electronic Engineers - International professional society that issues its own standards and is a member of the American National Standards Institute (ANSI) and the International Standards Organization (ISO); created IEEE Project 802.
IEEE 802.3	(In local area networking technology) Institute of Electrical and Electronic Engineers (IEEE) physical layer standard that uses the carrier sense multiple access with collision detection (CSMA/CD) access method on a broadcast bus topology local area network (LAN) commonly known as Ethernet.
ISO/OSI Reference Model	International Standards Organization Open Systems Interface seven-tiered network model
kbps	Thousands of bits per second (bps).

Local Area Network (LAN)	A computer and communications network that covers a limited geographical area, allows every node to communicate with every other node, and does not require a central node or processor
Network Interface Card (NIC)	Circuit Card required in the expansion bus of a workstation to provide connection to the LAN
TCP/IP	Transmission Control Protocol/Internet Protocol, a protocol created for the Department of Defense to innerconnect dissimilar computer systems.
X.25	Consultative Committee International on Telegraphy and Telephony (CITT) recomendation that defines the standard communications protocol for access to packet data networks (PDNs).
X.400	Consultative Committee International on Telegraphy and Telephony (CCITT) recommendation that defines message handling systems; used for E-mail systems.

3.0 NETWORK BACKBONE CONFIGURATION

In accordance with OPNAV guidance the network backbone standard will be implemented using a total fiber optic approach. Figure 3.1 depicts the standard configuration for a fiber optic LAN. The following paragraphs describe the components of the system in detail.

3.1 NETWORK INTERFACE CARDS

The Network Interface Card (NIC) used to provide connectivity of end user devices to the LAN must conform to the ULANA standard for the electronics side of the board. The boards shall be compatible with IEEE 802.3 standards and must be capable of supporting TCP/IP. Each NIC must provide an onboard or external fiber optic interface. The NIC can be interfaced to the fiber either via an onboard fiber optic modem or external fiber optic modem. Connection to the onboard modem is to be accomplished utilizing ST fiber optic connectors. Connection to the external modem is by DB-15 (DIX) connector.

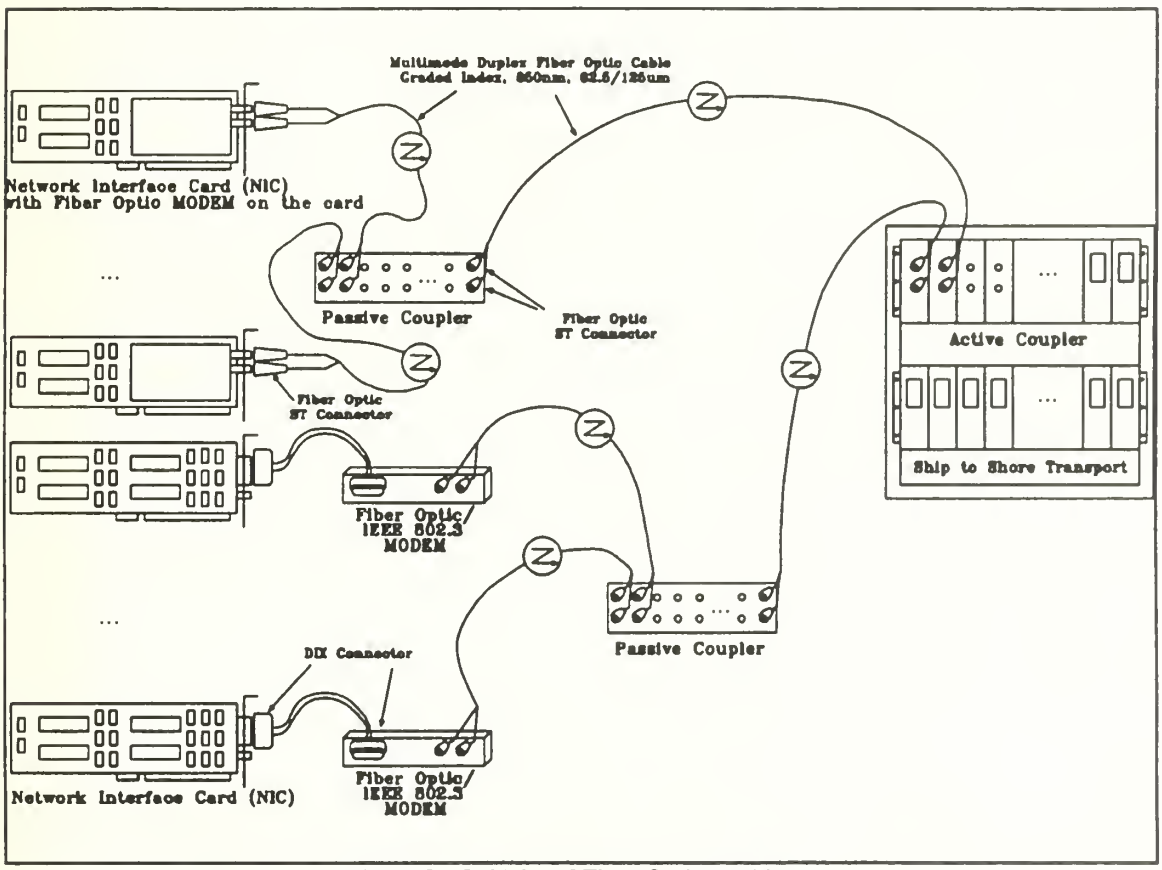


Figure 3.1 IMA LAN Fiber Optic Backbone

3.2 PASSIVE COUPLERS

Passive couplers are used for signal distribution to all stations in the LAN. These couplers must have no electronic components to fail and can be utilized to support installations of at least 150 meter connection lengths. Passive couplers to be utilized in approved installations must be completely fiber optic cable compatible with a minimum of seven input to seven outputs. Connectors on the passive couplers should be fiber optic ST connectors.

3.3 ACTIVE COUPLERS

Active couplers to be utilized in approved installations must be chassis based and can be standard 19" rack mountable or desktop. The power supply provided with the unit must be 115v UL approved with full capacity to support all slots in the unit without upgrading. The active unit must be capable of accepting repeater modules.

Repeater modules must support IEEE 802.3 standards. In order to support existing

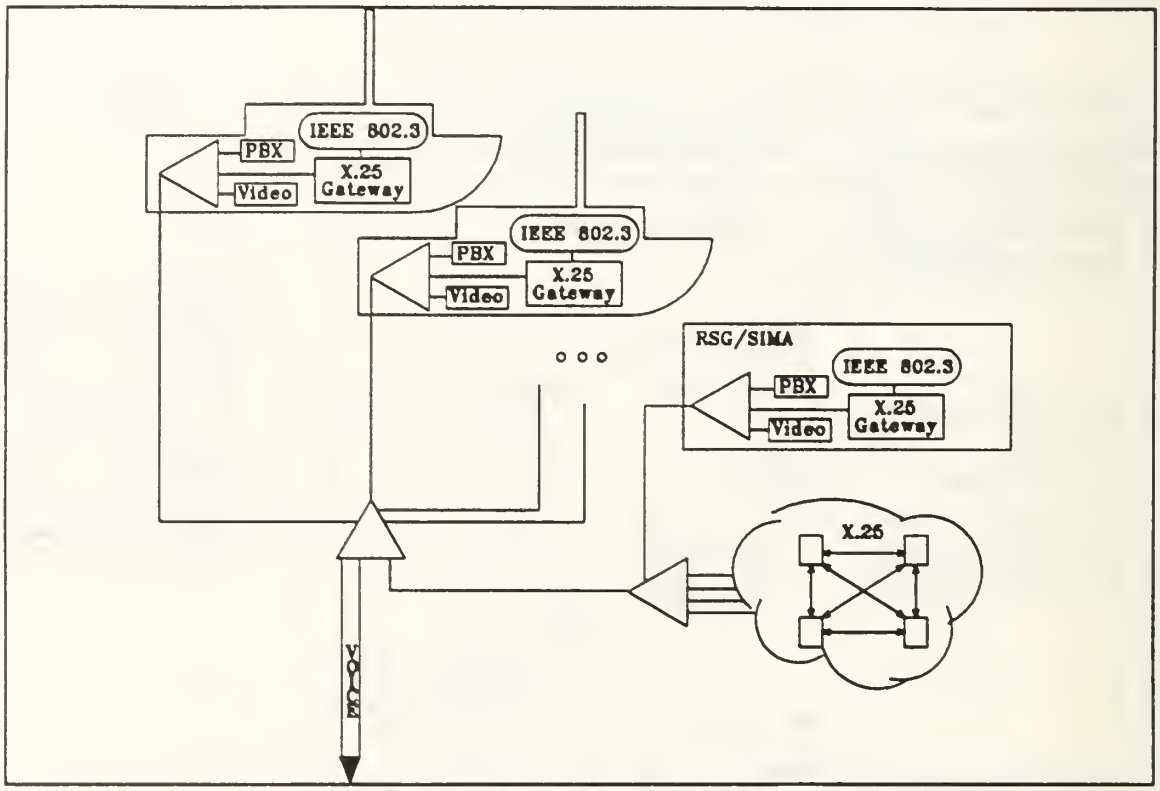


Figure 3.2 IMA LAN Telecommunications Plan

installed networks, the repeater modules must be capable of being utilized with the following mediums: thick coax, thin coax, twisted pair or fiber optic.

3.4 GATEWAY UNITS

Gateway units will be used as protocol converters and routers. The units must maintain a minimum of 32 virtual circuits. The gateway will be physically attached to the LAN and transmit data to the ship to shore transport unit. The gateway unit must be capable of providing X.25 protocol output.

3.5 SHIP TO SHORE TRANSPORT UNITS

Offsite Transport Units to be utilized in approved installations must be chassis based. The units must have the capability for simultaneous input from voice (PBX), video and data. The units must have fiber optic output capability.

3.6 CABLE/CONNECTORS

The approved cabling for LAN Backbone installations will utilize a 2 strand multi-mode fiber optic cable. The multi-mode cable will be 62.5/125 µm, graded index, with a wavelength of 850 nm and use a ST connector.

4.0 NETWORK FILE SERVER CONFIGURATION

4.1 HARDWARE CONFIGURATION

4.1.1 EXISTING FILE SERVER

Existing file servers to be attached to the backbone must be able to be upgraded to support TCP/IP and IEEE 802.3.

4.1.2 INITIAL IMA ADMINISTRATIVE LAN FILE SERVER

The network file server will be a Desktop III specified advanced workstation configured with the following options:

* (2) 300 Megabyte Hard Disk Storage Devices
* 16 MB RAM
* Monochrome Display and controller
* (2) Parallel Ports
* (4) Serial Ports

All hardware selected must be certified to operate with the selected LAN Operating system software. Systems not procured from Desktop III should coincide with the Desktop III configurations and options.

4.2 NETWORK OPERATING SYSTEM

Network Operating System must support the IEEE 802.3 standard and have the capability of supporting TCP/IP protocol for data transfer.

5.0 END USER DEVICES

5.1 END USER CENTRAL PROCESSING UNITS

5.1.1 EXISTING END USER CENTRAL PROCESSING UNITS

Existing end user devices to be attached to the generic PC-LAN can be any Central Processing Unit that is capable of supporting TCP/IP and IEEE 802.3.

5.1.2 INITIAL END USER CENTRAL PROCESSING UNIT SUPPLIED

The end user configuration for IMA Shipboard Administrative LAN will be as follows:

* DESKTOP III Basic Workstation with 2 MB RAM
* VGA 14" Color monitor and controller
* 41.9 MB Hard Disk Drive
* MS DOS 4.01
* TCP/IP Software compatible with the selected Network Interface Card

5.2 FUTURE ADDITIONS

Additions to the original installation will be required to meet the requirements of section 5.1.2.

6.0 IMA ADMINISTRATIVE LAN

6.1 HARDWARE REQUIREMENTS

The IMA Administrative Local Area Network installations must meet the standards previously defined. The initial hardware configuration will be as follows:

* (1) Network backbone configuration per Section 3.0
* (1) Network file server per Section 4.0
* (29) Initial End User devices per Section 5.2

Peripherals to be provided will include the following:

* (1) Desktop III Contract 340 MB Tape Cartridge Backup System
* (2) HP-LASERJET III capable of supporting HPGL and HPDL
* (3) HP-LASERJET IID capable of supporting HPDL on 2-sided paper

Devices may be added to the initial configuration as defined and supported by the requesting unit and approved by NAVSEA PMS-331.

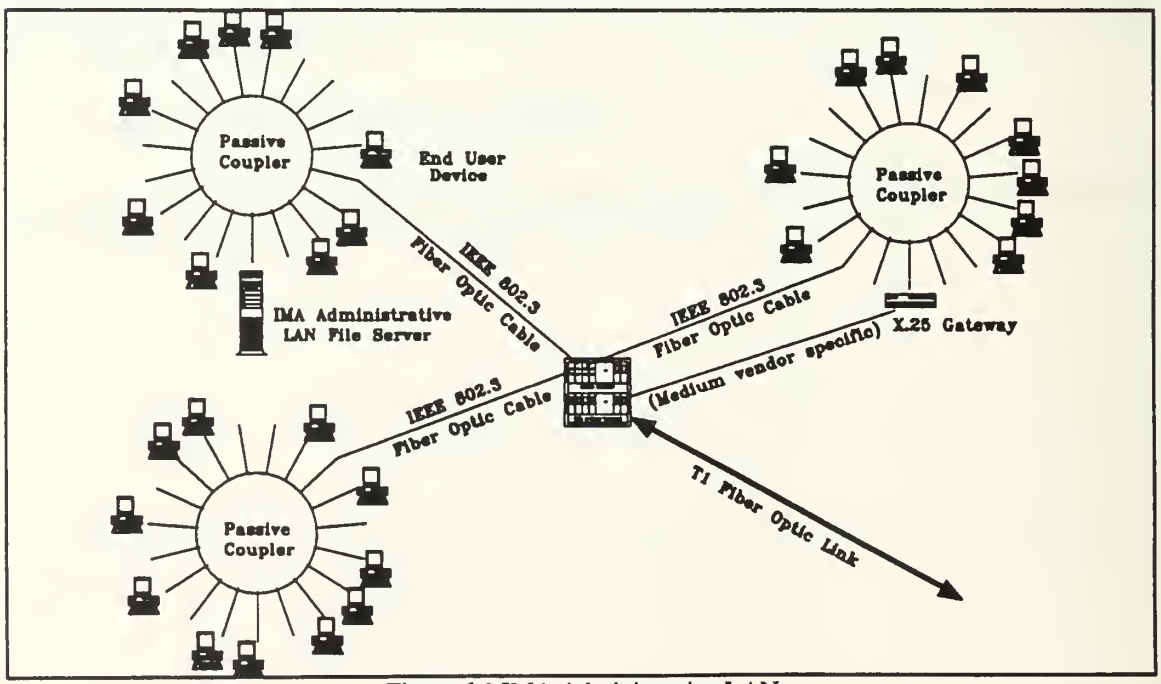


Figure 6.1 IMA Administrative LAN

6.2 SOFTWARE REQUIREMENTS

The IMA Administrative LAN Server will have the following software configuration:

Operating System Software

* Novell Netware/386 Operating System

Application Software

* Word Perfect 5.1
* QuattroPro
* Fox Pro
* Timeline 4.0
* Harvard Graphics
* X.400 Compliant (Electronic Mail)
* SABERMENU
* SABER METER
* TCP/IP compatible with the selected network interface card

Other software can be added to the server as defined by the request and approved by NAVSEA PMS-331.

6.3 PLACEMENT

The equipment placement for the IMA Administrative LAN will vary by installation. End user devices will be distributed throughout the repair departments to support the administrative requirements of the department. A minimum of 4 stations will be placed in locations which will allow maximum exposure of the resources for self-paced training. The location of the remaining stations will be determined during the site survey.

Additional nodes to an IMA Administrative LAN can be added as defined and supported by the requester and approved by NAVSEA PMS-331.

6.4 RESPONSIBILITIES

6.4.1 LAN ADMINISTRATOR

The ship must designate a single individual who will have responsibility for the administration of the network when the installation is complete. This individual will be responsible for adding and deleting new users, maintaining system availability and to act as a central point of contact for repairs and maintenance and scheduling of new user training. This individual should be assigned to the repair department. It is recommended that the candidate for this assignment be an ET, E-5 or above.

6.4.2 TRAINING

NAVSEA PMS-331 will provide training for users and the LAN system administrator concurrent with the installation of the network. Additional training classes will be available at Shore Intermediate Maintenance Activities.

6.4.3 MAINTENANCE

Maintenance and repair of the installed equipment will be the responsibility of the IMA.

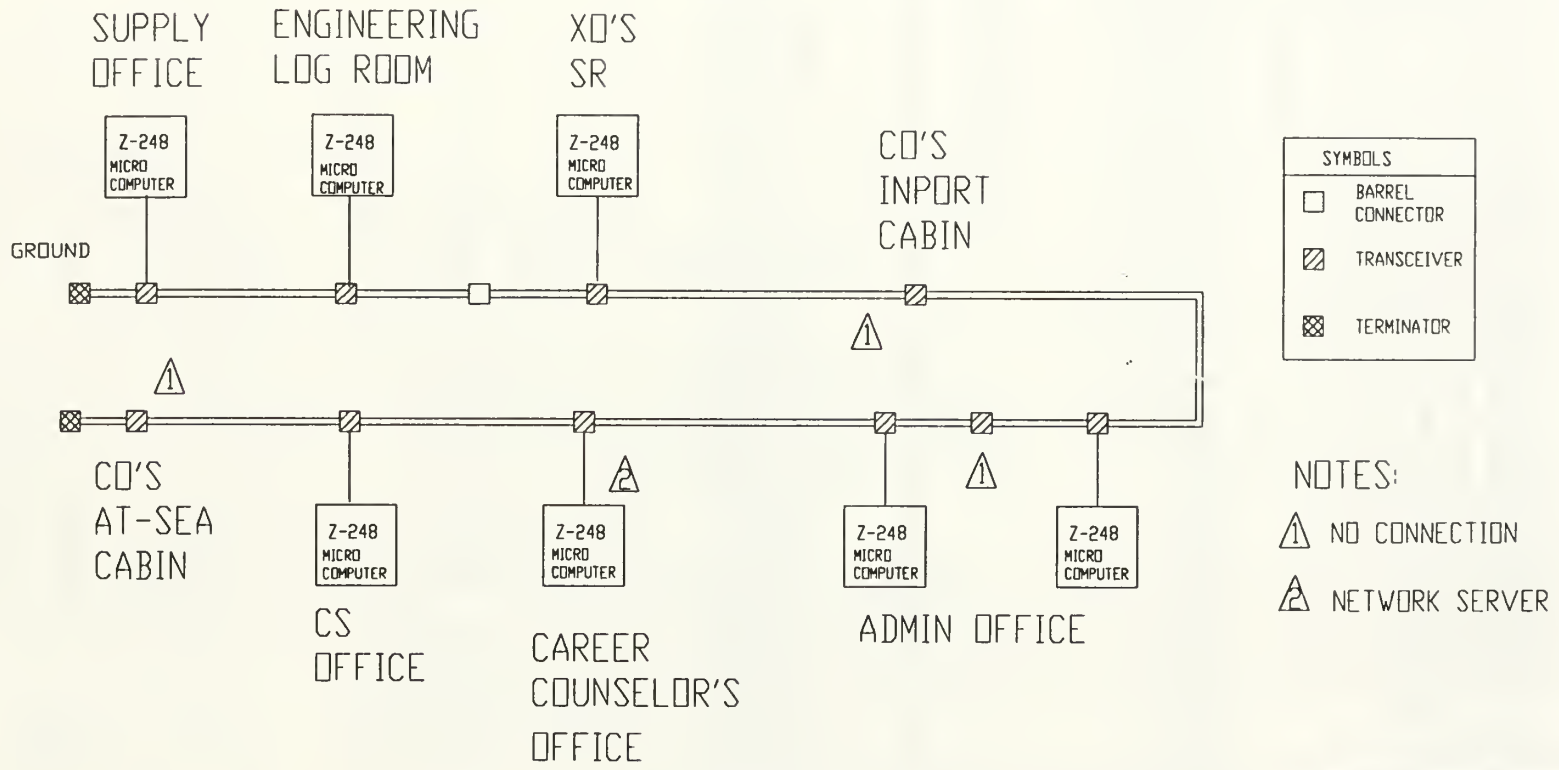
NAVSEA PMS-331 will have responsibility for approval of modifications or upgrades to the IMA Shipboard Administrative File Server Software. The IMA designated LAN Administrator will be responsible for installing approved upgrades/modifications.

PARTS LIST

QTY	PART NR	DESCRIPTION
700	1	CABLE, COAXIAL, IEEE 802.3 10BASE5 TYPE TFE
200	2	CABLE, 4 PAIR, TYPE TFE
4	3	CONNECTOR, TYPE N, MALE,
1	4	ADAPTER, TYPE N, DOUBLE FEMALE
10	5	TRANSCEIVER, IEEE 802.3, ISOLAN
10	6	CONNECTOR, DB15, MALE
10	7	CONNECTOR, DB15, FEMALE
7	8	IEEE 802.3 INTERFACE CARD, 3-COM
2	9	TERMINATOR, 50 OHM, TYPE N FEMALE
20	10	HOOD, DB15, SHIELDED METALLIC
10	11	SLIDE LOCK SET
10	12	SLIDE LOCK STAND OFF SET
1	13	GROUND CLAMP

CONTRACT NO.		
APPROVALS	DATE	TITLE
DRAWN	1/8/89	LAN INSTALLATION
		SIZE A
		NOT TO SCALE SHEET OF

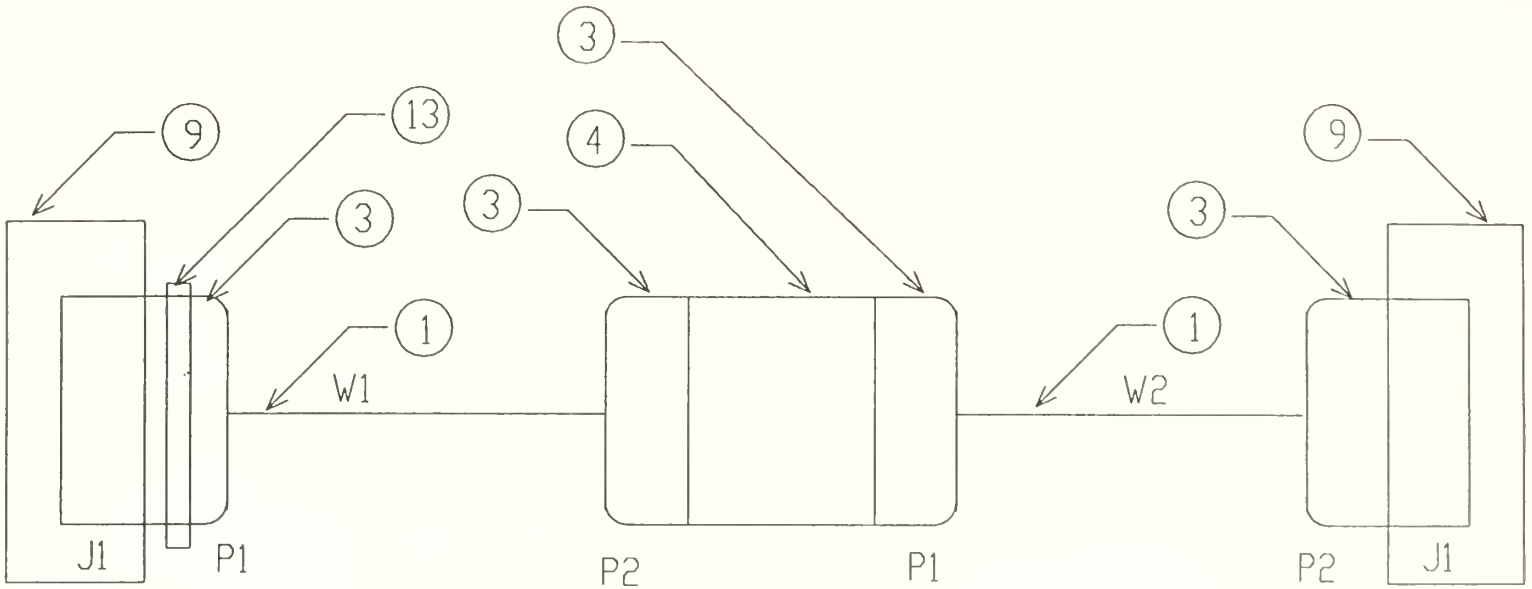
SYSTEM BLOCK DIAGRAM



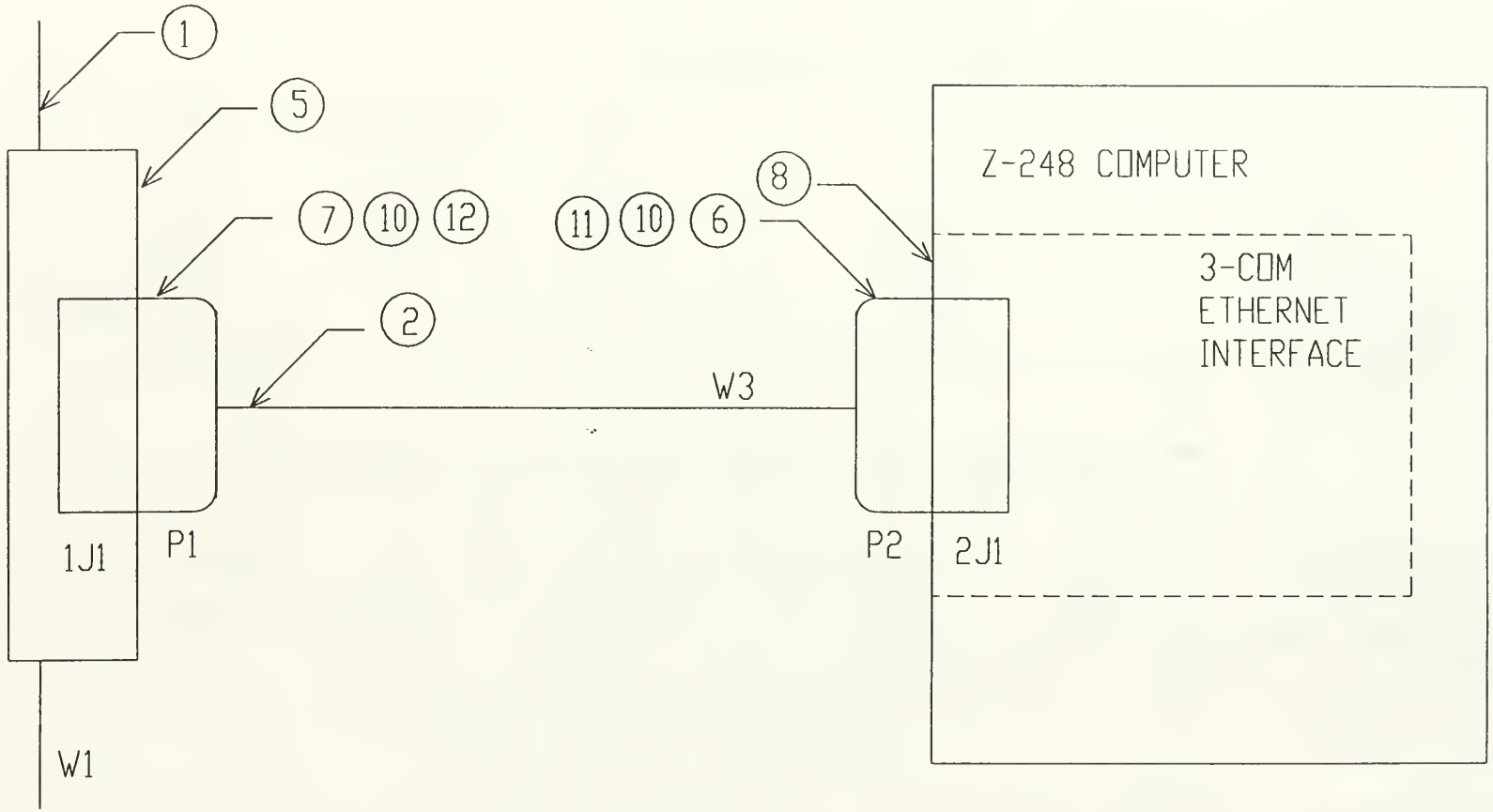
CONTRACT NO.		
APPROVALS	DATE	TITLE
DRAWN	1/9/89	LAN INSTALLATION
		SIZE A
		NOT TO SCALE SHEET OF

90

ETHERNET COAXIAL CABLE ASSEMBLY

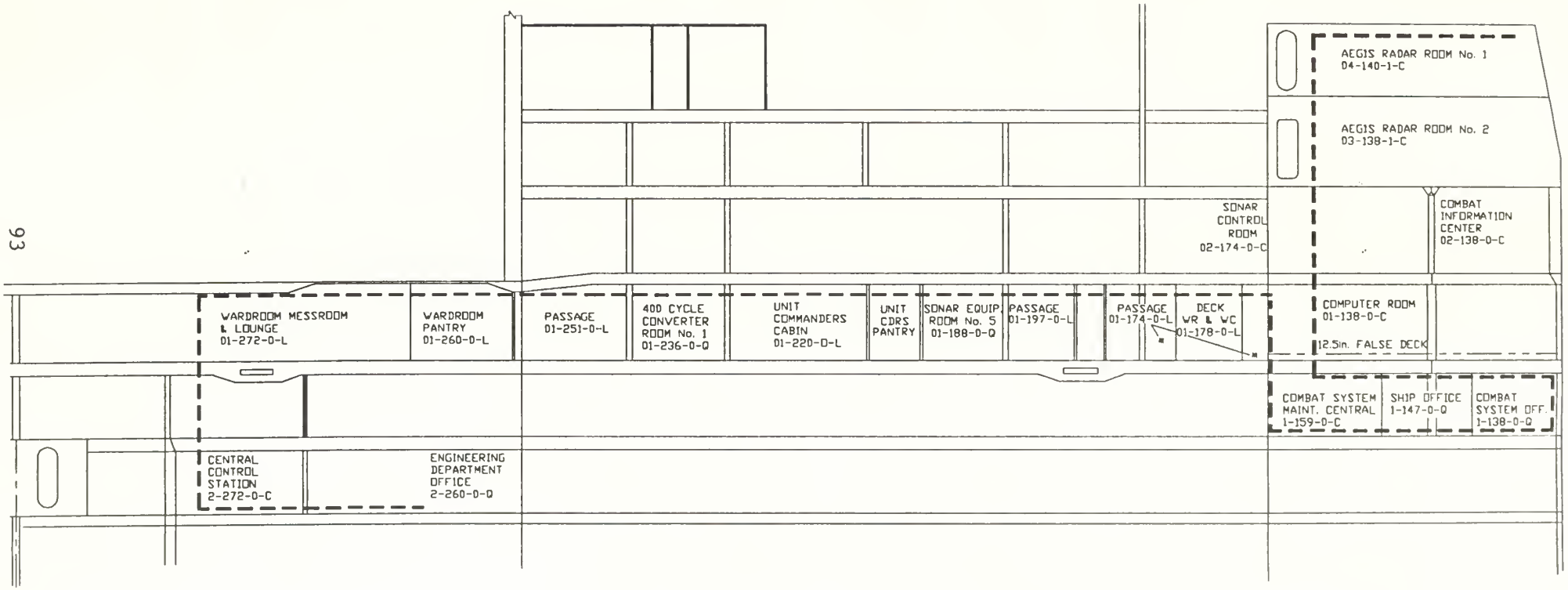


CONTRACT NO.		
APPROVALS	DATE	TITLE
DRAWN	1/9/89	LAN INSTALLATION
		SIZE A
		NOT TO SCALE SHEET OF



TRANSCEIVER INSTALLATION DETAIL

CONTRACT NO.		
APPROVALS	DATE	TITLE
DRAWN	1/8/89	LAN INSTALLATION
		SIZE A
		NOT TO SCALE
		SHEET OF


AEGIS RADAR ROOM No. 1
04-140-1-C
AEGIS RADAR ROOM No. 2
03-138-1-C
SONAR CONTROL ROOM
02-174-0-C
COMBAT INFORMATION CENTER
02-138-0-C
WARDROOM MESSROOM & LOUNGE
01-272-0-L
WARDROOM PANTRY
01-260-0-L
PASSAGE
01-251-0-L
400 CYCLE CONVERTER ROOM No. 1
01-236-0-Q
UNIT COMMANDERS CABIN
01-220-0-L
UNIT CDRS. PANTRY
SONAR EQUIP. ROOM No. 5
01-188-0-Q
PASSAGE
01-197-0-L
PASSAGE
01-174-0-L
DECK WR & WC
01-178-0-L
COMPUTER ROOM
01-138-0-C
12.5in. FALSE DECK
COMBAT SYSTEM MAINT. CENTRAL
1-159-0-C
SHIP OFFICE
1-147-0-Q
COMBAT SYSTEM OFF.
1-138-0-Q
CENTRAL CONTROL STATION
2-272-0-C
ENGINEERING DEPARTMENT OFFICE
2-260-0-Q

APPENDIX G

3COM MODEL 3C107 TRANSCEIVER

Signalling:	half-step signalling as required by 802.3 standard
Voltage:	2 KV RMS isolation voltage between the transceiver drop cable and the Ethernet cable as required by 802.3 standard
Cable length:	cable segment range of up to 1,000 meters (3,280 feet) for thick coaxial cable
MTBF:	observed Mean Time Between Failure rate of 2.9 million hours (330 years)

Transceiver Dimensions:

Length:	15.2 cm (6 in.)
Width:	3.2 cm (1.25 in.)
Height:	9.5 cm (3.75 in.)
Weight:	467 gm (15 oz.)

Warranty:	3COM warranty states that the 3C107 transceiver will be in good working order for three years after purchase from 3COM or an authorized 3COM reseller.

R 120730Z MAR 90

FM NARDAC NORFOLK VA//CODE 30//

TO AIG ONE ONE ZERO THREE NINE ACCT NA-CRAXDA

BT
UNCLAS //N05230//

SUBJ: DESKTOP III (DT3) CONTRACT; F01620-90-D-0001

1. REQUEST WIDEST DISSEMINATION.

2. UNISYS CORP WAS AWARDED THE DT3 MICROCOMPUTER CONTRACT ON 17 NOV 89. DT3 PROVIDES A SOURCE FOR 80386 DOS AND UNIX BASED DESKTOP SYSTEMS, SOFTWARE, AND ASSOCIATED PERIPHERALS.

3. NO PERSONAL BUY (PURCHASE OF SYSTEMS BY GOVT EMPLOYEES FOR PERSONAL USE) IS BEING OFFERED BY UNISYS AT THIS TIME. QUESTIONS CONCERNING PERSONAL BUYS SHOULD BE DIRECTED TO UNISYS.

4. UNISYS DT3 SUPPORT:
A. UNISYS TOLL FREE NUMBERS ARE ACCESSIBLE WITHIN CONUS, ALASKA, AND HAWAII. CALLS WILL BE ANSWERED BY THE FIRST AVAIL UNISYS ANALYST.
B. UNISYS TECH SUPPORT CENTER (HARDWARE/SOFTWARE/MAINTENANCE): TOLL FREE 1-800-468-3832, COMM1-205-244-2896. UNISYS ORDER TRACKING CENTER: TOLL FREE 1-800-247-3832, COMM 1-205-244-2897.
C. UNISYS ON-LINE BULLETIN BOARD SYSTEM: TOLLFREE 1-800-228-3832, COMM 1-205-244-2898. PROTOCOLS: KERMIT, XMODEM, OR SEALINK. BAUD RATES: 300, 600, 1200, 2400. PARAMETERS: 1 STOP, 8 DATA, NO PARITY.
D. DDN ACCESS AND OCONUS TECH SUPPORT WILLBE ESTABLISHED WITHIN THE NEXT 60 (SIXTY) DAYS.

5. WHILE SUPPORT FOR THE INSTALLED DOS BASED Z-248 MICROCOMPUTER IS AN IMPORTANT NAVY CONCERN, THE DT3 CONTRACT DID NOT REQUIRE COMPONENT INTEROPERABILITY. TESTS WILL BE RUN BETWEEN THE UNISYS PRODUCTS AND THE Z-248 TO DETERMINE THEIR COMPATIBILITY. THE RESULTS WILL BE PROVIDED VIA MESSAGE AS SOON AS THEY ARE AVAILABLE. USE OF DT3 PRODUCTS WITH THE Z-248 MAY VOID UNISYS' WARRANTY AND MAINTENANCE RESPONSIBILITY FOR THOSE ITEMS.

6. NARDAC NORFOLK POC IS TECH SUPPORT, CODE 311.1, A/V 565-2111 OR COMM 804-445-2111.
BT

APPENDIX I

VIRUS CHARACTERISTICS LIST V6.2

The following list outlines the critical characteristics of the known IBM PC and compatible viruses identified by SCAN.

Infects Fixed Disk Partition Table----------+
Infects Fixed Disk Boot Sector----------+ |
Infects Floppy Diskette Boot ----------+ | |
Infects Overlay Files----------+ | | |
Infects EXE Files----------+ | | | |
Infects COM files----------+ | | | | |
Infects COMMAND.COM----------+ | | | | | |
Virus Remains Resident----------+ | | | | | | |
Virus Uses Self-Encryption----------+ | | | | | | | |
| | | | | | | | |
| | | | | | | | | Increase in
| | | | | | | | | Infected
| | | | | | | | | Program's
| | | | | | | | | Size
| | | | | | | | | |
| | | | | | | | | |
Virus | Disinfector | V | V | V | V | V | V | V | V | V | Damage

Virus	Disinfector										Increase in Infected Program's Size	Damage
Kennedy	CleanUp	.	X	.	X	.	.	.	.	.	3088	D,F,L
Eight Tunes (1971)	CleanUp	.	X	.	X	X	X	.	.	.	1971	D,F,L
Yankee Doodle-2	CleanUp	.	.	.	X	X	.	.	.	.	1961	D,F,L
June 16th	CleanUp	.	.	X	X	.	.	.	.	.	1726	F,D,F,L
XAI	CleanUp	X	.	.	X	.	.	.	.	.	1539	F,D,F,L
1392	CleanUp	.	X	X	X	X	.	.	.	.	1392	D,F,L
1210	CleanUp	.	X	.	X	.	.	.	.	.	1210	D,F,L
1720	CleanUp	.	X	.	X	X	X	.	.	.	1720	F,D,F,L
Saturday 14th	CleanUp	.	X	.	X	X	X	.	.	.	685	F,D,F,L
Korea	M-DISK	.	.	.	.	.	.	X	X	.	N/A	B,D
Vcomm	CleanUp	.	.	.	.	X	.	.	.	.	1074	D,F,L
ItaVir	CleanUp	.	.	.	.	X	.	.	.	.	3880	D,F,L,B
Solano	CleanUp	.	X	.	X	.	.	.	.	.	2000	D,F,L
V2000	CleanUp	.	X	X	X	X	X	.	.	.	2000	D,F,L
1554	SCAN/D	.	X	X	X	X	.	.	.	.	1554	D,F,L
512	SCAN/D	.	X	X	X	.	.	.	.	.	none	D,F,L
EDV	M-DISK	.	X	.	.	.	.	X	X	X	N/A	B,D
Joker	CleanUp	.	X	X	X	.	.	.	.	.		D,F
Icelandic-3	CleanUp	.	X	.	.	X	.	.	.	.	853	D,F
Virus-101	CleanUp	X	X	X	X	X	X	X	X	.	2560	F
1260	CleanUp	X	.	.	X	.	.	.	.	.	1260	F
Perfume	CleanUp	.	.	.	X	.	.	.	.	.	765	F
Taiwan	CleanUp	.	.	.	X	.	.	.	.	.	700	F
Chaos	HDISK	.	X	.	.	.	.	X	X	.	N/A	B,D,D,F
Virus-90	CleanUp	.	X	.	X	.	.	.	.	.	857	F
Dropax	CleanUp	.	X	.	X	.	.	.	.	.	2773	F,D
4096	CleanUp	.	X	X	X	X	X	.	.	.	4096	D,D,F,L
Devil's Dance	CleanUp	.	X	.	X	.	.	.	.	.	941	D,D,F,L
Amstrad	CleanUp	.	.	.	X	.	.	.	.	.	847	F
Payday	CleanUp	.	X	.	X	X	X	.	.	.	1000	F
Datacrime II-B	CleanUp	X	.	X	X	X	.	.	.	.	1917	F,F
Sylvia/Holland	CleanUp	.	.	.	X	.	.	.	.	.	1332	p
Do-Nothing	CleanUp	.	X	.	X	.	.	.	.	.	600	p
Sunday	CleanUp	.	X	.	X	X	X	.	.	.	1636	D,F

Lisbon	CleanUp	. . . x	648	F
Typo/Fumble	CleanUp	. x . x	867	D,F
Dbase	CleanUp	. x . x	1864	D,D,F
Ghost Boot Version	MBISK	. x . . . . x x .	N/A	B,D
Ghost COM Version	CleanUp	. . . x	2351	B,F
New Jerusalem	CleanUp	. x . x x x . . .	1808	D,F
Alabama	CleanUp	. x . . x	1360	D,F,L
Yankee Doodle	CleanUp	. x . x x	2885	D,F
2930	CleanUp	. x . x x	2930	F
Ashar	CleanUp	. x . . . . x . .	N/A	B
AIDS	CleanUp	. . . x	Overwrites Program	
Disk Killer	CleanUp	. x . . . . x x .	N/A	B,D,F,D,F
1536/Zero Bug	CleanUp	. x . x	1536	D,F
MIXI	CleanUp	. x . . x	1618	D,F
Dark Avenger	CleanUp	. x x x x x . . .	1800	D,F,L
3551/Sysiock	CleanUp	x . . x x	3551	F,D
VACSINA	CleanUp	. x . x x x . . .	1200	D,F
Ohio	MBISK	. x . . . . x . .	N/A	B
Typo (Boot Virus)	MBISK	. x . . . . x x .	N/A	D,B
Swap/Israeli Boot	MBISK	. x . . . . x . .	N/A	B
1514/Datacrime II	CleanUp	x . . x x	1514	F,F
Icelandic II	CleanUp	. x . . x	661	D,F
Pentagon	MBISK	. . . . . x . .	N/A	B
3000/Traceback	M-3000	. x . x x	3000	F
1168/Datacrime-B	CleanUp	x . . x	1168	F,F
Icelandic	CleanUp	. x . . x	642	D,F
Saratoga	CleanUp	. x . . x	632	D,F
400S	CleanUp	. . . x	Overwrites Program	
1704 Format	CleanUp	x x . x	1704	D,F,F
Fu Manchu	CleanUp	. x . x x x . . .	2000	D,F
1280/Datacrime	CleanUp	x . . x	1280	F,F
1701/Cascade	CleanUp	x x . x	1701	D,F
1704/CASCADE-B	CleanUp	x x . x	1704	D,F
Stoned/Marijuana	CleanUp	. x . . . . x . x	N/A	D,B,L
1704/CASCADE	CleanUp	x x . x	1704	D,F
Ping Pong-B	CleanUp	. x . . . . x x .	N/A	D,B
Den Zuk	MBISK	. x . . . . x . .	N/A	D,B
Ping Pong	CleanUp	. x . . . . x . .	N/A	D,B
Vienna-B	CleanUp	. . . x	648	F
Lehigh	CleanUp	. x x	Overwrites	F,F
Vienna/648	M-VIENNA	. . . x	648	F
Jerusalem-B	CleanUp	. x . x x x . . .	1808	D,F
Yale/Alameda	CleanUp	. x . . . . x . .	N/A	B
Friday 13th COM	CleanUp	. . . x	512	F
Jerusalem	CleanUp	. x . x x x . . .	1808	D,F
SURIV03	CleanUp	. x . x x x . . .		D,F
SURIV02	CleanUp	. x . . x	1488	D,F
SURIV01	CleanUp	. x . x	897	D,F
Pakistani Brain	CleanUp	. x . . . . x . .	N/A	B

Legend:

Damage Fields - B - Corrupts or overwrites Boot Sector
D - Affects system run-time operation
F - Corrupts program or overlay files
d - Corrupts data files
F - Formats or erases all/part of disk
L - Directly or indirectly corrupts file linkage

Size Increase - The length, in bytes, by which an infected program or overlay file will increase

Characteristics - x - Yes
. - No

Disinfectors - SCAN/D - VIRUSCAN with /D option
SCAN/D/A - VIRUSCAN with /D and /A options
MDISK/F - MDISK with "F" option
All Others - The name of disinfecting program

Note:

The SCAN /D option will overwrite and then delete the entire infected program. The program must then be replaced from the original program diskette. If you wish to try and recover an infected program, then use the

11 JUNE 1990

VIRUS CHECKLIST/PROCEDURES

1. Machine location _____

   User Name _____

2. Boot System and Go to DOS

3. Insert Virus detection disk into Drive A:

4. For hard drives: go to Drive A:

   Example: "SCAN C: /M /A

   This would scan all files on drive C:, replace the C: with D: or E: (for other hard drives).

   To scan floppy disks: Go to Drive A:

   Example: SCAN A: /MANY /A

   This would scan all files on a floppy disk in drive a:

   Note: By specifying "/MANY" as a parameter allows multiple floppy disks to be scanned.

5. If virus is found while running "SCAN" the virus type will be displayed, EXAMPLE [STONED].

6. Remove disk, insert virus detection disk:

   Example:

   Type A:CLEAN <DRIVE LETTER> [Virus Name] /a

   RUN THIS TWICE

7. After "CLEAN" run "SCAN" again to ensure virus was removed

8. Flag the PC with a small "Yellow Post-it" on top of the monitor.

List the deleted/cleaned files

1.	2.	3.
4.	5.	6.

LIST OF REFERENCES

Benbasat, I., Goldstein, D. K., and Mead, M., "The Case Research Strategy in Studies of Information Systems," MIS Quarterly, v. 11, September 1987.

Brewin, Bob, "Desktop III 386s Can't Act as Network Servers, But NARDAC Has Fix," Federal Computer Week, v. 4, no. 27, July 16, 1990.

Brookshear, J. Glenn, Computer Science: An Overview, 2nd ed., p. 6-10, The Benjamin/Cummings Publishing Company, Inc., 1988.

Bruce, Walter R. III, Using Enable/OA, Que Corporation, 1988.

Cash, James I., Jr., and others, Corporate Information Systems Management: Text and Cases, 2nd ed., Richard D. Irwin, Inc., 1988.

Cohen, A., and others, Teacher's Manual for Use with Effective Behavior in Organizations, Richard D. Irwin, Inc., 1980.

Commander, Naval Sea Systems Command, Serial 74, PMS 306/GAM, to Deputy Under Secretary of the Navy (Financial Management), Subject: Shipboard Non-tactical ADP Program (SNAP) II System Selection, February 25, 1982.

DeMaio, Harry B., "Viruses - A Management Issue," Computers and Security, v. 8, no. 5, p. 381-387, May 1989.

Dixon, Robert H., Management Principles to be Considered for Implementing a Data Base Management System Aboard U.S. Naval Ships Under the Shipboard Non-tactical ADP Program, Master's Thesis, Naval Postgraduate School, Monterey, CA, December 1982.

Durr, Michael, and Gibbs, Mark, Networking Personal Computers, Que Corporation, 1989.

Editor, "Virus Protection," PC Business Software, v. 15, no. 1, p. 9-11, January 1989.

Fox, Jackie, "Introduction to Local-Area Networks," PC Today, issue 8, v. 4, p. 14-24, August 1990.

Fox, Jackie, "Getting Started With A Network," PC Today, issue 11, v. 4, p. 13-17, November 1990.

Fox, Jackie, "Unraveling the LAN Mystery," PC Today, issue 11, v. 4, November 1990.

Harvey, D. F., and Brown, D. R., An Experimental Approach to Organization Development, 3rd ed., Prentice-Hall Inc., 1988.

Hawkins, Corrine C., "What Users Should Know About Computer Viruses," Telecommunications, p. 42-44, July 1989.

Highland, Harold Joseph, Dr., "The Marijuana Virus Revisited," Computers and Security, v. 8, no. 5, p. 369-377, May 1988.

Highland, Harold Joseph, Dr., "Protecting Hardware and Software," Computers and Security, v. 8, no. 5, p. 647-656, May 1988.

House Of Representatives Bill (H. R. 145), 100th Congress, 1st Session, January 6, 1987.

Jane's Fighting Ships 1990-91, 93rd ed., p. 742, Jane's Information Group Limited, 1990.

Lawrence, Bill, Using Novell Netware, Que Corporation, 1990.

Lee, A. S., "Case Studies as Natural Experiments," paper prepared for the Decision Sciences Institute, November 1986.

Liss, Stanley M., and O'Rourke, Shawn T., SNAP II: Training Administrative Enhancements, Master's Thesis, Naval Postgraduate School, Monterey, CA, September 1987.

Maher, John J., and Hicks, James O., "Computer Viruses: Controlled Nightmares," Management Accounting, p. 44-49, October 1989.

McMican, William J., and Richards, James J., Shipboard Non-tactical Computer Systems of the U.S. Navy, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1985.

Miles, M. B., and Huberman, A. M., Qualitative Data Analysis: A Source Book of New Methods, Sage Publications, 1984.

Moulton, P. D., and Stanley, Timothy S., Hard Disk Quick Reference, Que Corporation, 1989.

Navy Maintenance and Supply Systems Office, Norfolk, Virginia, and Maintenance and Supply Systems Office Detachment Pacific, San Diego, California, Subject: Integrated Functional Description for Shipboard Non-tactical ADP Program II Shipboard Data System (SNAP II SDS), March 1981.

Navy Management Systems Support Office, NAVMASSO Document No. X-2122-004, MG-001 A, Shipboard Nontactical ADP Program (SNAP) II, Shipboard Management Overview, Management Guide, Norfolk, VA, July 23, 1986.

OPNAV Instruction 5230.16, Subject: Fleet Non-tactical ADP Support Management Structure, July 10, 1978.

Pascale, R., "Direction of the NonDirective Method," Stanford University, Graduate School of Business, Summer 1973.

Pfaffenberger, Bryan, Ph.D., Que's Computer User's Dictionary, Que Corporation, 1990.

Powell, Joyce L., Prototype Development and Redesign: A Case Study, Master's Thesis, Naval Postgraduate School, Monterey, CA, March 1990.

Roberts, Ralph, Computer Viruses, COMPUTE! Books, 1988.

Rosenau, W., and Schumacher, M., "A Case For New Study Methods," Military Forum, v. 4, June 1988.

Ruff, David, LCDR, USN, "The Advent of the Paperless Ship," Naval Engineers Journal, v. 100, no. 4, July 1988.

U.S. Small Business Administration, SOP 80 05, MSB and COD Programs, p. 9-28, September 4, 1979.

Wiseman, Simon, "Preventing Viruses in Computer Systems," Computers and Security, vl. 8, no. 5, p. 427-431, May 1988.

Yin, R. K., Case Study Research Design and Methods, Sage Publications, 1976.

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5000	2
3.	Defense Logistics Studies Information Exchange (DLSIE) US Army Logistics Management Center Fort Lee, Virginia 23801	1
4.	William J. Haga, Code AS/HG Naval Postgraduate School Monterey, California 93943-5000	1
5.	Thomas P. Moore, Code AS/MR Naval Postgraduate School Monterey, California 93943-5000	1
6.	CDR Tom J. Hoskins, Code 37 Naval Postgraduate School Monterey, California 93943-5000	1
7.	LCDR Cheryl L. Gonzalez 6015 Pinetree Drive Shelby Township, Michigan 48316	2